

Certification and Accreditation Report

For The

**Defense Occupational and Environmental Health Readiness System
Data Repository
Version 1.5.1
(DOEHRS-DR 1.5.1)**

15 September 2004

	<p>MHS Advanced Technology Innovation Center Three Skyline Place - 5201 Leesburg Pike, Suite 1600 Falls Church, VA 22041</p>	 Health Affairs
---	---	--

For Official Use Only

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

REVISION AND HISTORY PAGE

Document Version #	Revision Date	Description of Change	Section # / Paragraph #	Page #

TABLE OF CONTENTS

1 INTRODUCTION	1
1.1 PURPOSE	1
1.1.1 Responsibility	2
1.1.2 Certification Activities.....	2
2 SCOPE	4
3 BACKGROUND	5
3.1 SYSTEM DESCRIPTION	5
3.1.1 DOEHRS-DR 1.5.1 Hardware / Software.....	6
3.1.2 System Interfaces and External Connections	7
3.1.3 System Criticality.....	8
3.1.4 Functional Description.....	9
3.2 VALIDATION OF FEDERAL REGISTER NOTICES	9
3.3 VALIDATION OF VCTS/VMS REGISTRATION	9
3.4 VALIDATION OF PORTS AND PROTOCOLS.....	9
3.5 VALIDATION OF PERSONNEL SECURITY (IT STATUS)	10
3.6 CERTIFICATION LEVEL	10
4 SECURITY REQUIREMENTS	12
5 SECURITY EVALUATION	13
5.1 AUTOMATED VULNERABILITY SCAN	13
5.2 RISK ASSESSMENT ACTIVITIES	13
5.2.1 Documentation Review.....	13
5.2.2 Technical Control Features Assessment	14
5.2.3 Security Features Demonstration/Testing	14
5.3 EVALUATION FINDINGS	14
6 RISK ASSESSMENT SUMMARY	25
6.1 COMPLIANCE DETERMINATION CRITERIA.....	25
6.2 EVALUATION RESULTS.....	26
6.3 CONCLUSIONS AND RECOMMENDATIONS	26

LIST OF TABLES

TABLE 1: DOEHRS-DR 1.5.1 SERVER SOFTWARE.....	6
TABLE 2: DOEHRS-DR 1.5.1 CONNECTION REQUIREMENTS.....	7
TABLE 3: DOEHRS-DR 1.5.1 PORTS AND PROTOCOLS	10
TABLE 4: DOEHRS-DR 1.5.1VULNERABILITY MATRIX.....	17
TABLE 5: DOEHRS-DR 1.5.1 SSAA DOCUMENTATION COMPLIANCE	25

LIST OF FIGURES

FIGURE 1: DOEHRS-DR 1.5.1 ARCHITECTURE	4
FIGURE 2: DOEHRS-DR 1.5.1 DATA FLOW	8
FIGURE 3: DOEHRS-DR 1.5.1 TEST REPORT	15

LIST OF ATTACHMENTS

ATTACHMENT A: ACRONYMS

ATTACHMENT B: REQUIREMENTS TRACEABILITY MATRIX

EXECUTIVE SUMMARY

This report has been developed for the Joint Medical Information Systems Office / Military Health Systems (JMISO/MHS) Designated Approving Authority (DAA) by the JMISO Certification Team to document the level of risk to the currently accredited Defense Occupational and Environmental Health Readiness System – Data Repository, Version 1.5.1 (DOEHRS-DR 1.5.1). An Approval to Operate (ATO) for a period of three years was granted to DOEHRS-DR on 20 July 2001. On 16 June 2003, the Military Health System (MHS) Information Assurance (IA) Program published the Periodic Review for DOEHRS-DR 1.5.1. MHS IA confirmed that there had been no major changes in the system and that sufficient security measures were in place to permit the DOEHRS-DR 1.5.1 ATO to remain in effect until 21 July 2004. Because of the recent migration of DOEHRS-DR 1.5.1 from the Clinical Information Technology Program Office (CITPO) to the Resources Information Technology Program Office (RITPO), the current ATO was extended to 15 September 2004 to permit sufficient time for proper testing and mitigation of risks.

DOEHRS-DR 1.5.1 is corporate module of a multifaceted system known as DOEHRS. The DOEHRS is an Automated Information System (AIS) designed to support the Occupational Health (OH) program within the Military Health System (MHS). The Department of Defense (DoD) OH program supports the prevention of illness and injury to DoD military members and civilian employees from exposure to chemical, biological, or physical hazards. DOEHRS-DR 1.5.1 is used by DoD occupational and environmental health professionals distributed across Army, Navy, Air Force, and National Guard facilities to query, analyze, abstract, and report information about individual exposures to hazards in the workplace.

DOEHRS-DR 1.5.1 is managed by the Resource Information Technology Program Office (RITPO), administered by the DOEHRS Program Management Office (PMO) and housed at the U.S. Army Center for Health Promotion and Preventive Medicine (CHPPM) at the Aberdeen Proving Ground (APG) in Maryland.

The DOEHRS-DR 1.5.1 functions as the long-term storage repository of corporate OH data and is designed to serve the needs of the OH professional and command personnel by providing reporting and decision support services for immediate and future needs of the DoD, including:

- Data Reporting, using generated reports for decision-making analysis
- Data analysis, using Commercial Off-the-Shelf (COTS) Web-enabled report generation tools to provide a variety of reports
- Data manipulation, using various techniques for data aggregation, consolidation, and presentation

DOEHRS-DR 1.5.1 is in Phase III of the System Life Cycle: Production and Deployment.

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

DOEHRS-DR 1.5.1 has been designated as a Mission Assurance Category, Level Two (MAC II) Sensitive system on 25 August 2003.

During the evaluation period the following security test and evaluation events occurred:

IA Controls Assessment for MAC II Sensitive System

DOEHRS-DR 1.5.1 is a MAC II Sensitive system, handling information that is important to the support of deployed and contingency forces. Consequences of loss of integrity are unacceptable, and the loss of availability can be tolerated only for a short period of time. Department of Defense Instruction 8500.2, "*Information Assurance (IA) Implementation*", (DoDI 8500.2), requires compliance with threshold controls for systems, including DOEHRS-DR 1.5.1 as a MAC II Sensitive system.

A DoDI 8500.2 assessment was conducted on 18 June 2004, and resulted in the identification of six (6) DOEHRS-DR 1.5.1 vulnerabilities, each rated as Low risks. Following a review of mitigation activities by the JMISO Certification and Accreditation Team on 24 August 2004, no findings were closed, and the six vulnerabilities remain Low risks.

Certification Testing and Evaluation

On 29 June 2004, the JMISO Certification Team conducted Certification Testing and Evaluation (CT&E) scans on the DOEHRS-DR 1.5.1 servers residing at the CHPPM in Maryland.

The initial CT&E of DOEHRS-DR 1.5.1 resulted in 73 findings by the JMISO Certification Team. Thirteen (13) findings were deemed High risks, thirty-nine (39) findings were considered Medium risks, and twenty-one (21) findings were designated as Low risks. After DOEHRS-DR 1.5.1 completed mitigation activities, the initial findings were re-evaluated by the JMISO Certification Team and reduced to one (1) Medium risk and four (4) Low risks. These results are reflected in the following tables, which distinguish vulnerabilities and risk ratings for:

- The IA Controls Assessment for MAC II Sensitive systems
- The DOEHRS-DR 1.5.1 servers at the CHPPM

Initial Findings

	High	Medium	Low	Total
DOEHRS-DR 1.5.1 Servers CHPPM, APG	13	39	21	73
IA Control Testing & Assessment			6	6
Total	13	39	27	79

DOEHRS-DR 1.5.1 Certification and Accreditation Report

After mitigation activities were completed, the initial findings were re-evaluated on 16 August 2004, and the JMISO Certification Team determined that the findings have been reduced to the risks indicated in the table, below.

Post-Mitigation Findings

	High	Medium	Low	Total
DOEHRS-DR 1.5.1 Servers CHPPM, APG		1	4	5
IA Control Testing & Assessment			6	6
Total		1	10	11

The results of all testing are included in the body of this report.

For the purposes of this Certification and Accreditation, remaining risks are classified either as residual risks or short-term risks. These risks are identified and classified in the appropriate sections of this report:

Residual Risks: The risks that remain in the operation of DOEHRS-DR 1.5.1 after all possible cost-effective mitigations have been applied. These risks are acceptable to the DAA with the understanding that DOEHRS-DR 1.5.1 will seek to further resolve these vulnerabilities throughout the system life cycle and at the earliest possibility.

Short-Term Risks: Security deficiencies identified in DOEHRS-DR 1.5.1 that the DAA does not intend to accept as permanent risks, but is willing to accept for a minimal period of time because of the system's mission criticality. These risks must be addressed and resolved immediately, and the DAA will assign a completion date for each short-term risk based upon the nature of the individual risk. A system's failure to close a short-term risk may result in the withdrawal or amendment of the DAA's accreditation decision.

The Certification Team has determined that, with the closure of all short-term risks, DOEHRS-DR 1.5.1, will have satisfied DoD and MHS baseline security requirements and should be granted an Approval to Operate (ATO). Vulnerabilities have been mitigated by DOEHRS-DR 1.5.1 and the JMISO Certification Team validated mitigation results. There are eleven (11) remaining vulnerabilities identified as residual or short-term risks; one (1) is a Medium risk and ten (10) are Low risks. Of these remaining risks, four (4) are designated as short-term risks, and the remainder are considered acceptable residual risks. The Certifying Authority (CA) recommends to the Designated Approving Authority (DAA) that an ATO be granted under the following terms and conditions:

General Conditions:

- a. If the Resources Information Technology Program Office (RITPO), otherwise known as the Program Office (PO), makes any changes to the configuration of DOEHRS-DR 1.5.1, the PO

DOEHRS-DR 1.5.1 Certification and Accreditation Report

must assess and document the impact on the security policies and processes. This involves fully understanding any changes that are made to the security policies and processes, documenting any new vulnerability, conducting elimination or mitigation to reduce risk, and finally updating the System Security Authorization Agreement (SSAA) and supporting documents. The JMISO Certification Team must be notified, and provided a copy of the updated security documents.

b. The PO must use the following guidelines in determining the level of certification activities required when changes are made to the configuration of DOEHRS-DR 1.5.1, baseline:

- 1) If the PO deems the changes to the configuration to be “minor”, the changes can be documented using Release Notes that have a security section. An example of a “minor” change would be the addition of functional changes that do not make any changes to the security policies and procedures.
- 2) If the PO deems the changes to the configuration to be more than “minor” but still less than a “major” change, a Risk Assessment must be coordinated with and validated by the JMISO Certification Team. The results normally will be documented as an addendum to the system accreditation report. An example of this type of change would be the addition of a new Commercial-Off-The-Shelf (COTS) product to the application or, adding one or more new interfaces to the system.
- 3) If the PO deems the changes to the configuration to be a “major” change, then a full Certification and Accreditation effort that leads to a new Approval to Operate (ATO) must be performed by the JMISO Certification Team. Examples of “major” changes include changing the operating system, or changing a major component, such as the database used by the system.

c. Mitigation of the system’s technical risks, identified under “Specific Conditions” below, are not to be delayed for the duration of the approved certification, but rather completed by the PO as quickly as resources permit.

2. Specific Conditions:

The CA recommends that the PO complete the following mitigation activities to further reduce the risk to the PO:

- Take all appropriate actions to close the Medium risk indicated in this report, or reduce this risk to a Low rating and to the extent that it may be considered an acceptable residual risk to the operation of DOEHRS-DR 1.5.1. The JMISO Certification Team and DOEHRS-DR 1.5.1 will coordinate efforts, prior to 01 December 2004, to allow JMISO verification that this task is completed
- Establish and document a procedure to ensure that the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA), including Appendices, is reviewed and updated as necessary upon any significant change to the system security or configuration and, at least, on an annual basis. DOEHRS-DR 1.5.1 will validate this action to the JMISO Certification Team prior to 01 December 2004

DOEHRS-DR 1.5.1 Certification and Accreditation Report

- Initiate efforts to establish an alternate site for DOEHRS-DR 1.5.1 at a location physically separate from APG in Aberdeen, Maryland

3. Other:

Best practices and JMISO policy will require DOEHRS-DR 1.5.1 to resolve any relevant issues relating to the upcoming discontinuation of Microsoft support of Windows NT. Although not considered a risk for the purposes of this Certification and Accreditation, these circumstances create a business risk because systems will be removed from Service networks if Windows NT is running and unsupported.

It is recommended that the DAA require that all of the above conditions be satisfied as soon as possible and no later than the next Annual Review for DOEHRS-DR 1.5.1.

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

DISCLAIMER

The use of trade names and references to specific equipment in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report, in presenting the success or failure of one (or several) part number(s), model(s), under specific environments and output requirements, does not imply that other products not herein reported on are either inferior or superior. This document may not be cited for advertising purposes.

DOEHRS-DR 1.5.1 Certification and Accreditation Report

1 INTRODUCTION

This Accreditation Report informs Resources Information Technology Office (RITPO) as well as the Designated Approving Authority (DAA) of the current state of the Defense Occupational and Environmental Health Readiness System – Data Repository, Version 1.5.1 (DOEHRS-DR 1.5.1) security posture.

RITPO develops, operates, and maintains automated information systems to support managing the resources of the TRICARE Management Activity, TRICARE Regional Lead Agent offices, and Service Surgeon General offices.

The focus of the Military Health System (MHS) is on the patient; however, to achieve excellence across the enterprise, many necessary business processes must perform properly. The RITPO plays a central role in providing many of the key capabilities that ensure the MHS runs smoothly. RITPO delivers information technology systems that help military treatment facilities optimize manpower and personnel, collect and track provider credential information; automate third party payments for outpatient insurance billing; and determine the total cost of providing health care to beneficiaries. RITPO provides information technology solutions for optimizing personnel and financial resource management throughout the MHS. The collection of Occupational Health (OH) data by DOEHRS-DR 1.5.1, with ensured integrity, availability and confidentiality, assists RITPO in meeting these goals.

An Approval to Operate (ATO) for a period of three years was granted for DOEHRS-DR 1.5.1 on 20 July 2001. On 16 June 2003, the MHS Information Assurance (IA) Program (MHS IA) published the Periodic Review for DOEHRS-DR 1.5.1. MHS IA confirmed that there had been no major changes in the system and that sufficient security measures were in place to permit the DOEHRS-DR 1.5.1 ATO to remain in effect until 21 July 2004. Because of the recent migration of DOEHRS-DR 1.5.1 from the Clinical Information Technology Program Office (CITPO) to the Resources Information Technology Program Office (RITPO), the current ATO was extended to 15 September 2004 to permit sufficient time for proper testing and mitigation of risks.

This report describes the safeguards provided by the DOEHRS-DR 1.5.1 designs to ensure that the system is operated and managed in compliance with Department of Defense (DOD) security requirements throughout its life cycle. This report also describes applicable security requirements, summarizes key security evaluation activities supporting accreditation, and makes recommendations regarding accreditation.

1.1 Purpose

The purpose of the security evaluation was to determine the extent to which DOEHRS-DR 1.5.1 technical security controls and documentation meet the minimum DoD and MHS system security requirements for an ATO. The security evaluation provides the framework necessary to build a basis for Certification and Accreditation (C&A) of DOEHRS-DR 1.5.1 according to DoD Directive 8500.1, “*Information Assurance*.” The DoD Directive 8500.1 requires that

DOEHRS-DR 1.5.1 Certification and Accreditation Report

accreditation, which is granted by the system's DAA, be supported by a technical evaluation of system security safeguards.

1.1.1 Responsibility

The RITPO is responsible for the project management and overall life cycle management of DOEHRS-DR 1.5.1. The MHS Security Policy mandates that DOEHRS-DR 1.5.1 undergo the "DoD Information Technology Security Certification and Accreditation Process" (DITSCAP) evaluation. The DITSCAP ensures that adequate security measures have been implemented to enable the system to maintain the required level of trust within an authorized operational environment. The JMISO Certification Team assumed responsibility for certification of DOEHRS-DR 1.5.1 on 19 April 2004. Full certification and accreditation, with the granting of an Approval to Operate (ATO) by the DAA, must be undertaken every three years, or prior to expiration of an IATO. A system also must re-certify when the accredited safeguards are significantly affected due to system changes or updates, or if the operational environment has been significantly changed. DOEHRS-DR 1.5.1 requires a re-certification due to the expiration of the current ATO on 20 July 2004 (extended by the DAA until 15 September 2004). The Periodic Review was conducted by the MHS IA confirmed that there had been no major changes in the system and that sufficient security measures were in place to permit the DOEHRS-DR 1.5.1 ATO to remain in effect until its expiration.

1.1.2 Certification Activities

The principal activities conducted by the Certification Team in support of C&A include a review of the System Security Authorization Agreement (SSAA), performance of a security evaluation, security testing, and evaluation of the life cycle management processes. The JMISO Certification and Accreditation activities consisted of a review of available DOEHRS-DR 1.5.1 documentation, interviews with government and contractor personnel, security testing, and observations of demonstrated security features. Each activity is summarized in the sections below.

1.1.2.1 System Security Authorization Agreement

The DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA) was prepared in accordance with the DOD 8510.1-M, "*DoD Information Technology Security Certification and Accreditation Process Application Manual*".

The DOEHRS-DR 1.5.1 SSAA and associated appendices were reviewed for compliance against DOD 8510.1-M and to ensure that the DOEHRS-DR 1.5.1 and its security controls are correctly and completely represented in the system documentation.

1.1.2.2 Security Evaluation

A baseline security evaluation was conducted to identify potential threats to the system, the system's vulnerabilities, and the safeguards needed to reduce risks. The evaluation also determined the extent of compliance with security requirements of DoD and MHS. It consisted of a review of available DOEHRS-DR 1.5.1 documentation, interviews with appropriate personnel, and observations of demonstrated security features.

1.1.2.3 Security Testing

Security testing was performed to validate the effectiveness of the DOEHRS-DR 1.5.1 security features and capabilities. The system was tested utilizing Internet Systems Security (ISS) Internet Scanner™ and Systems Scanner™ using the Defense Information Systems Agency (DISA) Field Security Office (FSO) full Policy “v621xpu640” and Windows 2000 Systems Readiness Review (SRR) scripts. Manual tests were performed utilizing DODI 8500.2 MAC II Sensitive system Information Assurance (IA) Controls and the Network Infrastructure Security Checklist version 4, release 2.3. The test results indicate whether technical and procedural safeguards are implemented to ensure an acceptable level of risk to justify an Approval to Operate (ATO) or Interim Approval to Operate (IATO).

1.1.2.4 Life Cycle Security Management

DoD 5000.1, “*Life Cycle Management*” requires management procedures to be in place to ensure the maintenance of DOEHRS-DR 1.5.1 system security features and capabilities throughout the system life cycle.

The DOEHRS-DR 1.5.1 system stores and processes sensitive medical data. Such data is required to be safeguarded against unauthorized use by the DoD Privacy Act Program as well as Section 1102, Title 10, U.S. Code, entitled “*Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants*” (10 U.S.C. 1102) in cases where it provides a peer review or assessment regarding the quality of care. In accordance with criteria established by the Computer Security Act of 1987, the DOEHRS-DR 1.5.1 system is classified as a system that processes Sensitive Unclassified information because of the nature of the data it processes. The data in DOEHRS-DR 1.5.1 requires appropriate technical, procedural, physical, and operational safeguards to ensure its continuing confidentiality, integrity, and availability. Management procedures are in place to ensure the maintenance of DOEHRS-DR 1.5.1 security throughout the system's life cycle.

The DOEHRS-DR 1.5.1 system is in the Phase III, Production, Fielding/Deployment and Operational Support life-cycle phase.

2 SCOPE

This security evaluation analyzes the security risks associated with the overall DOEHRS-DR 1.5.1 system and its environment. The DOEHRS-DR 1.5.1 combined security protection mechanisms enforce the unified system security policy and establish the DOEHRS-DR 1.5.1 Trusted Computer Base (TCB). The TCB defines the system's accreditation boundary. This security evaluation only addresses elements within that boundary and assumes that equipment outside the boundary operates correctly, and those security procedures implemented outside the boundary are adequate. Figure 1 depicts the DOEHRS-DR 1.5.1 architecture with the accreditation boundary as described in the DOEHRS-DR 1.5.1 SSAA shaded in the right portion of the diagram.

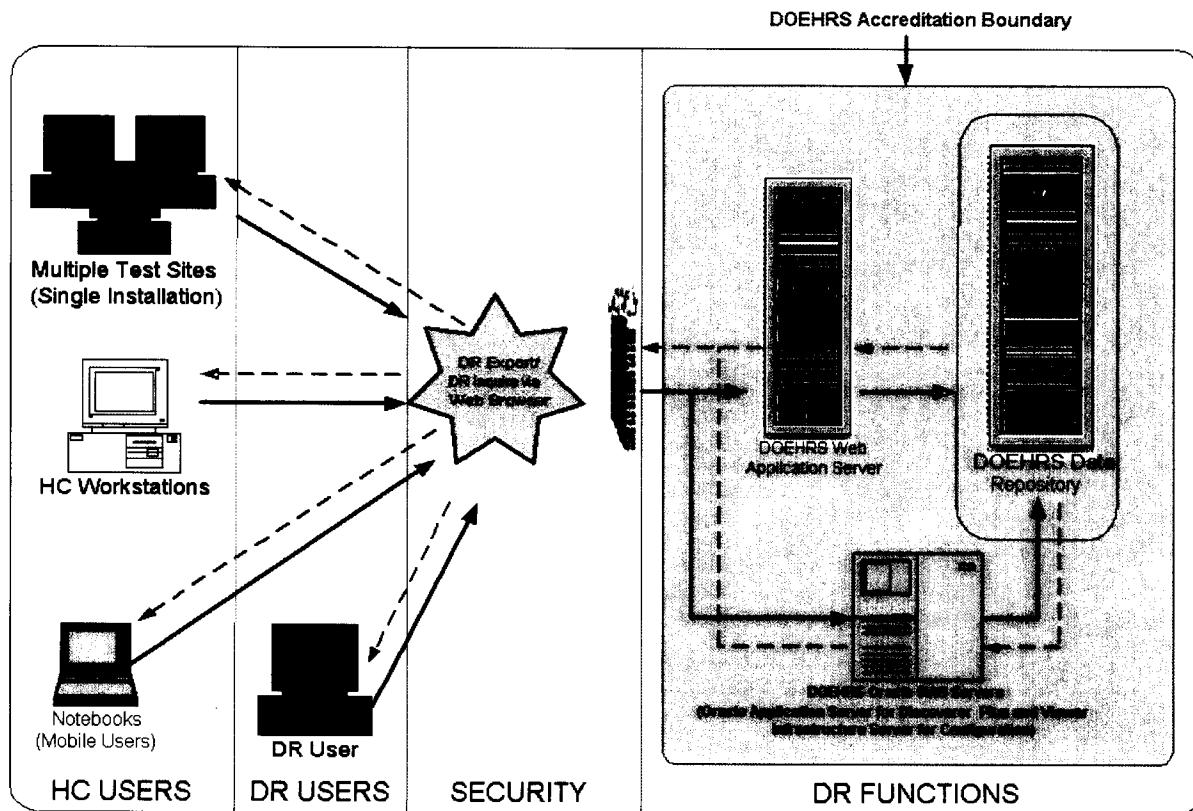


Figure 1: DOEHRS-DR 1.5.1 Architecture

3 BACKGROUND

The following information has been extracted from the DOEHRs-DR 1.5.1 SSAA documentation, and has been organized and edited to comply with the format requirements of this report.

3.1 SYSTEM DESCRIPTION

DOEHRs is a comprehensive, Tri-Service Automated Information System (AIS) for collecting, comparing, processing, evaluating, and storing occupational exposure information, selected baseline medical examination data, workplace environmental monitoring data, personal protective equipment usage data, observation of work practices data, and employee health hazard education data. DOEHRs supports the OH mission and enhances readiness. It also provides timely and efficient access of data and information to users throughout the DoD worldwide including Military Treatment Facility (MTF) commanders, industrial site commanders, lead agents, installation agencies, and other users of comprehensive OH information.

DOEHRs improves the quality of OH care and wellness programs for the DoD workforce by promoting the equitable delivery of OH services and the development of more robust and informed prevention programs to minimize the impact of worksite hazards. Readiness benefits are recognized from reduced troop retraining due to partial disability and improved unit fitness through exposure life cycle tracking. DOEHRs is an operational data collection system and a distributed database system. It replaces legacy service-specific applications and provides automated support where no automated information support existed previously. It supports reduction in redundant data entry and timely, efficient data sharing between hazardous work sites and OH clinics. DOEHRs supports elimination of redundant data collection through interfaces with clinical, environmental, safety, personnel, and financial AIS within DoD, as well as systems external to DoD, which provide federal standards and compliance information.

At the facilities where the OH data is collected, authorized personnel input into the Hearing Conservation (HC) modules using a variety of devices (e.g., pen-based workstations and desktops). HC data flows directly to the DOEHRs Web Server. This effectively establishes a single authoritative source of reference data for operational processing. The Web Server is located at the Center for Health Promotion and Preventive Medicine (CHPPM) Data Center, but is managed by the DOEHRs Technical Integration Office (TIO). Data required to support online analytical or decision support processing flows to the DOEHRs DR Staging Area on the DR Production Server where it is transformed and then loaded to the DOEHRs-DR 1.5.1. Data loaded to the DOEHRs-DR 1.5.1 is aggregated to support the Decision Support System (DSS) capability where needed. The data is transferred using batch methodology, on a periodical, non-real-time basis. Recovery of recent data is possible and designed into DOEHRs-DR 1.5.1 architecture.

Exposures may occur throughout the continuum of military operations, such as industrial maintenance facilities, administrative offices, hospitals, aboard ship, while operating weapon systems in training exercises, or while deployed in war fighting or other military operations. The

DOEHRS-DR 1.5.1 Certification and Accreditation Report

DOEHRS-DR 1.5.1 enhances the ability to manage this reality by providing critical information to OH staff, command surgeons, and commanders so they can effectively select options for reducing health threats and conducting risk assessments. Authorized users access DOEHRS-DR 1.5.1 through an Internet browser. While these users may not modify data within DOEHRS-DR 1.5.1, they may request standardized documents for view or print. The ability to request these documents is based on the user's access level. These reports are used for operations management and decision support and are based on aggregated data.

3.1.1 DOEHRS-DR 1.5.1 Hardware / Software

The hardware configuration for DOEHRS-DR 1.5.1 is defined by DOEHRS Program Management Office (PMO) as any configuration meeting DoD requirements and service-specific regulations that is capable of running Web browser (IE 5.5, Netscape 7, or above), supporting 256 colors and JavaScript. End user workstation accreditation is the responsibility of the user's host network Information System Security Officer (ISSO) or the local security manager/commander. Based on these specifications, it is anticipated that the minimum configuration for a DOEHRS-DR 1.5.1 client is:

- Intel (Pentium II or Celeron) processor 400 megahertz (MHz) (or better)
- 128 megabyte (MB) Random Access Memory (RAM)
- 100 MB of free high density disk (HDD) space
- Network interface card
- Super Video Graphics Array (SVGA) video adapter.

The DOEHRS-DR 1.5.1 Server Software and Connection Requirements are described in Tables 1 and 2, below.

DOEHRS-DR 1.5.1 Server Software	Purpose	Type
Microsoft® Windows 2000 w/SP4	Server Operating System	COTS
Oracle8i™	Oracle® RDBMS Engine for DOEHRS-DR 1.5.1 data storage	COTS
Cold Fusion Version 6.1 (MX)	Report Server Engine—produces Web-ready report pages on demand and handles user session management	COTS
DOEHRS-DR 1.5.1 Main Application	Reporting Application for providing Functionals w/detailed statistics about HC field-testing.	PMO
Oracle 9i Application Server	Application Server for housing DOEHRS- DR applications	COTS

Table 1: DOEHRS-DR 1.5.1 Server Software

DOEHRS-DR 1.5.1 Client Software	Purpose	Type
Microsoft® Windows NT® Workstation 4.0 w/SP 6a or higher	Operating System	COTS
Microsoft® Windows XP® and Microsoft® Windows 2000 ®		
Internet Explorer 5.5 and higher or Netscape 7 and higher	Web browser with JavaScript-enabled setting	COTS

Table 2: DOEHRS-DR 1.5.1 Connection Requirements

3.1.2 System Interfaces and External Connections

The DOEHRS has one active interface with DOEHRS-HC (Hearing Conservation). The communication between the two TCBs is two-way, and initiated by the DOEHRS-HC users. DOEHRS-DR 1.5.1 is a central repository of information that receives data from DOEHRS-HC in the form of exports. The requested HC data is then uploaded into a staging area through the processing of batch files. Hearing specialists, who use a Government Off-the-Shelf (GOTS) product to conduct the administration of the hearing tests, create the export files. These export files are processed by the DBA who updates the DOEHRS-DR 1.5.1.

The data in the export files, which are loaded into DOEHRS-DR 1.5.1, consist of individual records for each test result. Data elements include personnel identification (ID) information, Major Command/Unit Identification Code (MACOM/UIC) designations, test data attributes, and administrator data.

The DOEHRS-HC can request records from the data repository through the DOEHRS-HC interface. Individual social security numbers (SSN) or Zip/Pas/UIC codes are passed to DOEHRS-DR 1.5.1 over a secure channel processed by the data repository and returned to DOEHRS-HC via the secure channel. Data elements include personnel ID information, MACOM/UIC designations, test data attributes, and administrator data.

3.1.2.1 DOEHRS-DR 1.5.1 Data Flow

Users may access the system's reports through a Web browser, (there is no other interface for the clients into the system). Users must log in with a unique user identification (Userid), password, and use a browser that supports security features. The specific protocol is Hypertext Transfer Protocol-Secure (HTTPS). Cold Fusion MX and Java are the communication vehicles that transport requests and information between the user, the web server and the Data Repository. The log-in request is processed by Oracle 8.i®, using standard services, and upon approval, a user is presented with the report selection menu. A graphical depiction of the data flow is presented in Figure 2, below.

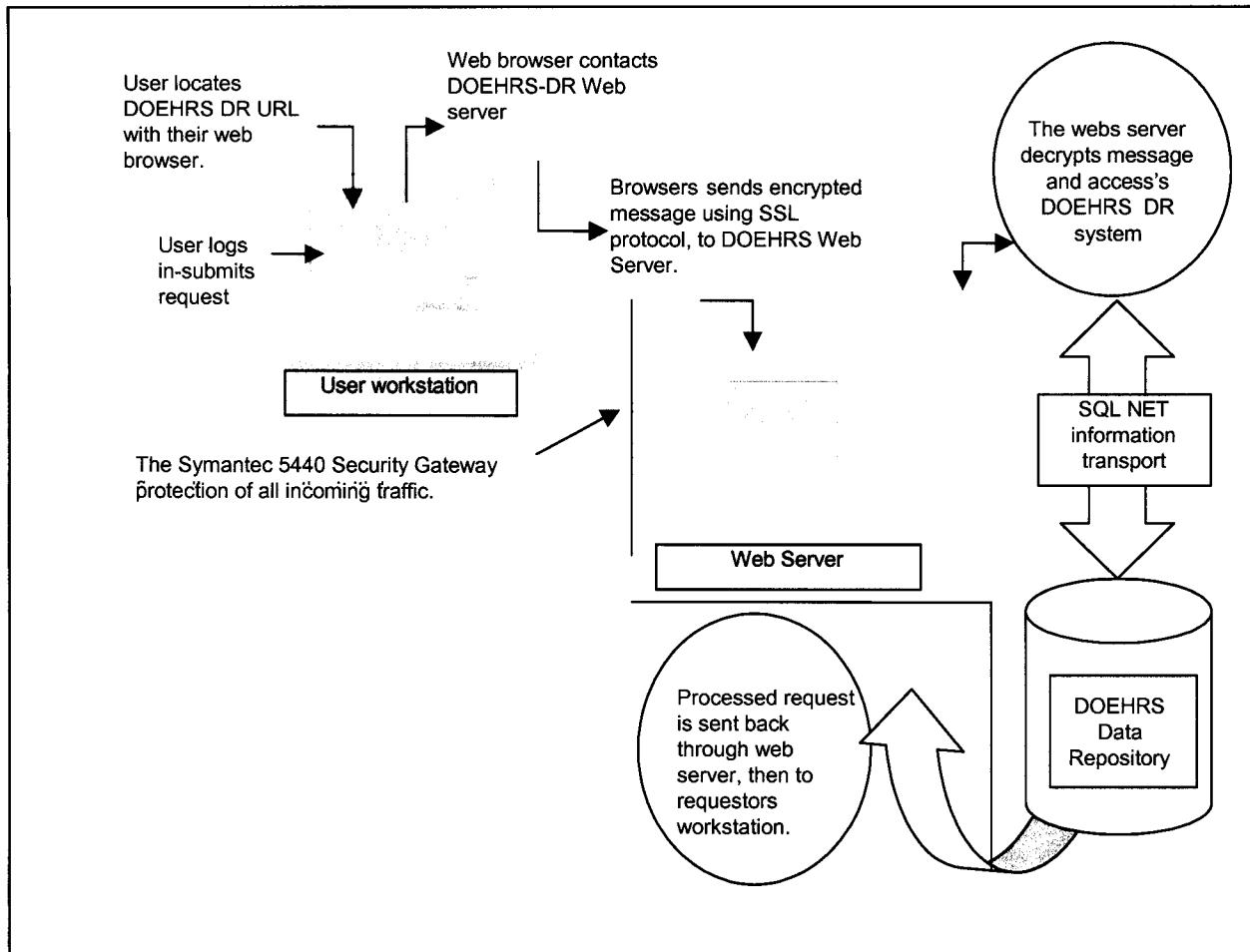


Figure 2: DOEHRSDR 1.5.1 Data Flow

3.1.3 System Criticality

The RITPO has classified DOEHRSDR 1.5.1 as a “Support” system, and defines the system as a “System handling sensitive information which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term.”

While users of the DOEHRSDR 1.5.1 depend on the system to provide accurate data, the timeliness of the data is not critical due to the addition of a real-time interface with the DOEHRSDR Hearing Conservation (HC) application. However, because DOEHRSDR 1.5.1 has been categorized as a MAC II Sensitive system, additional IA Controls and a more robust evaluation must be applied to satisfy MAC II compliance. As a MAC II Sensitive system, the loss of integrity to DOEHRSDR 1.5.1 is unacceptable, and loss of availability can be tolerated only for a short time.

DOEHRS-DR 1.5.1 Certification and Accreditation Report

3.1.4 Functional Description

The DOEHRS-DR 1.5.1 functions as the long-term storage repository of corporate OH data and is designed to serve the needs of the OH professional and command personnel by providing reporting and decision support services for immediate and future needs of the DoD.

DOEHRS-DR 1.5.1 system's capabilities include the following:

- Data Reporting, using prepared reports for decision-making analysis
- Data analysis, using Commercial Off-the-Shelf (COTS) Web-enabled report generation tools to provide a variety of canned reports
- Data manipulation, using various techniques for data aggregation, consolidation, and presentation.

3.2 VALIDATION OF FEDERAL REGISTER NOTICES

The Privacy Act of 1974, as amended, requires the publishing of a *Federal Register* notice of the existence and character of an automated System of Records containing Privacy Act data on individuals who are citizens of the United States or aliens lawfully admitted for permanent residency. These notices for DoD MHS systems are prepared by the system Program Manager and processed by the TMA Privacy Office in compliance with DoD Regulation 5400.11-R, *Privacy Program* dated August 1983. DOEHRS-DR 1.5.1 is in compliance with this requirement.

3.3 VALIDATION OF VCTS/VMS REGISTRATION

The Defense Information Systems Agency (DISA), as a DoD agency, is responsible for implementing the guidance and maintaining responsibility for the Information Assurance Vulnerability (IAVA) process throughout DoD. To support DISA's internal implementation of the IAVA process, DISA has developed the Vulnerability Compliance Tracking System (VCTS), a tool used to track compliance information for each DISA organization at the asset level. This is accomplished through the VCTS notice process. All information technology (IT) assets that are susceptible to vulnerabilities must be registered in the VCTS. Each asset must be registered with the component Vulnerability Management System (VMS) Point of Contact (POC) in order to expedite IAVA compliance. Program Offices are required to show proof of registration with the appropriate component POC. DOEHRS-DR 1.5.1 complied with this requirement prior to migration to RITPO from CITPO.

3.4 VALIDATION OF PORTS AND PROTOCOLS

Every AIS must register Ports and Protocols (PnP) with the appropriate POC. The POC is responsible for consolidating a list of AIS required by their organization, including the protocols and/or ports utilized, as well as operational and technical necessity for open ports. Each program office must show proof of prior registration (deployed systems) or planned registration if the AIS is a prototype. DOEHRS-DR 1.5.1 has registered the following Ports and Protocols.

Port	Protocol	Location	Direction
443 - 443	TCP/ HTTPS	Enclave to Internet	In
443 - 443	TCP/ HTTPS	Enclave to NIPRNet	In
443 - 443	TCP/ HTTPS	NIPRNet to Internet	In
443 - 443	TCP/ HTTPS	Enclave to Internet	Out
443 - 443	TCP/ HTTPS	Enclave to NIPRNet	Out
443 - 443	TCP/ HTTPS	NIPRNet to Internet	Out

Table 3: DOEHRS-DR 1.5.1 Ports and Protocols

3.5 VALIDATION OF PERSONNEL SECURITY (IT STATUS)

Any system that contains Privacy Act data is required to comply with DoD Regulation 5200.2-R, “*Personnel Security Program*”. Specifically, Appendix 10 containing the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating IT and IT-related positions. The DOEHRS-DR 1.5.1 Program Manager has supporting documentation in the SSAA and has taken appropriate steps to ensure that all personnel under RITPO control have appropriate Automatic Data Processing/Information Technology (ADP/IT) investigations in place or under way and, as such, are in compliance with DOD 5200.2-R.

3.6 CERTIFICATION LEVEL

The determination of Certification level requires the analysis of the following factors as applied to DOEHRS-DR 1.5.1:

- System business function
- National, DoD and MHS security requirements
- Criticality of DOEHRS-DR 1.5.1 to the MHS mission

DOEHRS-DR 1.5.1 Certification and Accreditation Report

- Software products
- Computer Infrastructure
- Data processed
- Types of users

These factors are compared to the degree of confidentiality, integrity, availability, and accountability required for DOEHRS-DR 1.5.1 through application of weighted system characteristics established for DITSCAP in DoD Manual 8510.1-M, “*DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Application Manual*” at Section C3.4.8.2.

There are four possible certification levels:

- Level 1 – basic security review
- Level 2 – minimum analysis
- Level 3 – detailed analysis
- Level 4 – comprehensive analysis

Using the process described above, the JMISO C&A Team and RITPO concur that the appropriate certification level for the DOEHRS-DR 1.5.1 is Certification Level 2.

4 SECURITY REQUIREMENTS

DOEHRS-DR 1.5.1 is required to comply with the following guidance:

- DoD 5200.2-R, “*DoD Personnel Security Program*”, dated 1 January 1997 (with administrative re-issuances)
- DoD 5220.22-M, “*National Industrial Security Program Operating Manual*”, January 1995; Change 1, 31 July 1997; Change 2, 1 May 2000
- DoD 5220.22-M, Supplement 1, “*National Industrial Security Program Operating Manual Supplement*”, February 1995
- DoD 5220.22-R, “*Industrial Security Regulation*”, December 1985
- DoD 5400.7-R, “*Freedom of Information Act*” (FOIA)
- DoD 8510.1-M, “*Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*”, July 2000
- DoD Directive 8500.1, “*Information Assurance (IA)*”, 24 October 2002
- DoDD 5200.2, “*DoD Personnel Security Program*”, dated 9 April 1999
- DoDD 5400.11, “*DoD Privacy Program*”, dated 13 December 1999
- DoDI 8500.2, “*Information Assurance (IA) Implementation*”, 6 February 2003
- OMB Circular A-130, “*Management of Federal Information Resources (Transmittal Memorandum No. 4)*”, 30 November 2000
- Public Law 100-235, “*Computer Security Act of 1987*”, 8 January 1988
- Public Law 104-106 *Information Technology Management Reform Act*, Clinger-Cohen Act, 1996
- DoD Manual 8510.1-M, “*DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Application Manual*”, 31 July 2000
- Public Law 104-191, “*Health Insurance Portability and Accountability Act*”, 1996, (HIPAA)

5 SECURITY EVALUATION

The security evaluation identified security requirements and examined the DOEHRS-DR 1.5.1 technical and procedural safeguards and associated system documentation. The evaluation examined the configuration identified in this report. The objective was to determine the extent to which the DOEHRS-DR 1.5.1 system safeguards and security relevant documentation meets baseline security requirements.

For the purposes of this Certification and Accreditation, remaining risks are classified either as residual risks or short-term risks. These risks are identified and classified in the appropriate sections of this report:

Residual Risks: The risks that remain in the operation of DOEHRS-DR 1.5.1 after all possible cost-effective mitigations have been applied. These risks are acceptable to the DAA with the understanding that DOEHRS-DR 1.5.1 will seek to further resolve these vulnerabilities throughout the system life-cycle.

Short-Term Risk: Security deficiencies identified in DOEHRS-DR 1.5.1 that the DAA does not intend to accept as permanent risks, but he is willing to accept for a minimal period of time because of the system's mission criticality. These risks must be addressed and resolved immediately, and the DAA will assign a completion date for each short-term risk based upon the nature of the individual risk. A system's failure to close a short-term risk may result in the withdrawal or amendment of the DAA's accreditation decision.

5.1 AUTOMATED VULNERABILITY SCAN

In support of the certification process, components are scanned utilizing Internet Systems Security (ISS) Internet Scanner™ and Systems Scanner™ using the Defense Information Systems Agency (DISA) Field Security Office (FSO) full Policy "v621xpu640" and Windows 2000 Systems Readiness Review (SRR) scripts. Manual tests were performed utilizing DODI 8500.2 MAC II Sensitive system Information Assurance (IA) Controls and the Network Infrastructure Security Checklist version 4, release 2.3.. The automated scanning tools used were configured in accordance with National Security Agency (NSA) guidelines and the applicable DISA Security Technical Implementation Guide (STIG).

5.2 RISK ASSESSMENT ACTIVITIES

The security evaluation is a comparison of DoD application and system security requirements to the existing application security controls. The objective was to determine the extent to which the DOEHRS-DR 1.5.1 safeguards and security relevant documentation satisfy baseline security requirements.

5.2.1 Documentation Review

DOEHRS-DR 1.5.1 security documentation was reviewed to support the evaluation of implemented controls. Documentation included:

- System Security Authorization Agreement with Appendices
- System Security Concept of Operations

DOEHRS-DR 1.5.1 Certification and Accreditation Report

- Information System Security Policy
- Requirements Traceability Matrix
- Certification Test and Evaluation Plan
- Trusted Facility Manual
- Configuration Management Plan
- Security Features User's Guide
- System Rules of Behavior
- Incident Response Plan
- Contingency Plan
- Security Awareness and Training Plan
- Personnel Control Memorandum
- Memorandums of Agreement

5.2.2 Technical Control Features Assessment

A review of DOEHRS-DR 1.5.1 system technical control features was conducted to determine the existence and/or sufficiency of required controls. Information was obtained from available documentation and interviews with DOEHRS-DR 1.5.1 system and support personnel. DOEHRS-DR 1.5.1 system security mechanisms are designed to meet baseline-security requirements for a MAC II Sensitive classification.

5.2.3 Security Features Demonstration/Testing

Security testing of DOEHRS-DR 1.5.1 system was conducted between 29 June 2004 and 24 August 2004, and focused on the following areas:

- The protection of information from unauthorized access – confidentiality,
- Denial of service (availability)
- The integrity of the system and data (integrity) and,
- The ability to ensure that system events are traceable to persons or processes that may then be held responsible for their actions (accountability)

5.3 EVALUATION FINDINGS

DOEHRS-DR 1.5.1 was assessed between 19 April 2004 and 08 September 2004. The initial evaluation resulted in a total of seventy-nine (79) findings from the MAC II IA Control review and the Certification Testing and Evaluation (CT&E) of the application and database. These findings were rated as 13=High, 39=Medium and 27=Low. Further mitigation was conducted, issues were resolved and the system was reassessed by the JMISO Certification Team. After mitigation, eleven (11) remaining risks were identified and rated as one (1) Medium and ten (10) Low. Of these findings following mitigation by DOEHRS-DR 1.5.1, four (4) risks were deemed short-term risks, and the remainder were designated as residual risks.

Figure 3 depicts a graphical representation of identified vulnerabilities before and after mitigation.

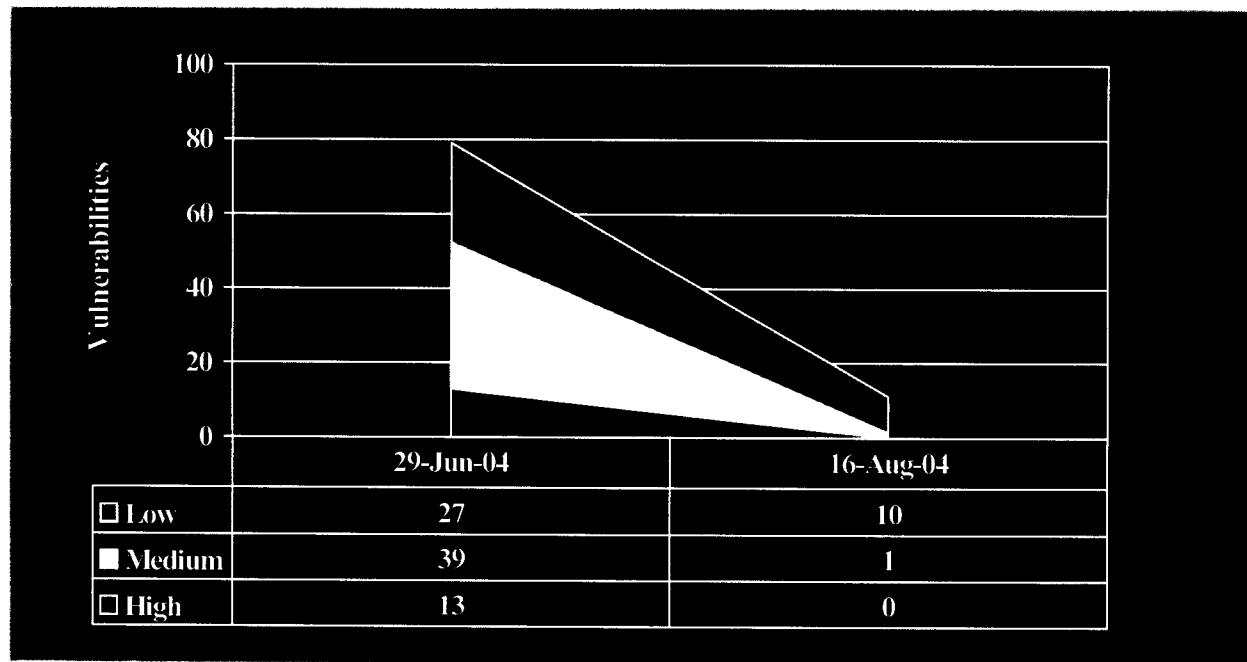


Figure 3: DOEHRS-DR 1.5.1 Test Report

Table 4 represents a matrix of identified vulnerabilities including:

- Risk rating of initial finding
- System area in which vulnerability was identified
- Vulnerability finding, including impact statement and recommendation
- Response or mitigation strategy developed by the Program Office (RITPO)
- Certification Team response to the Program Office
- Final Residual Risk rating following validation testing or analysis

The Vulnerability Matrix for DOEHRS-DR 1.5.1 aggregates several risks as a single issue. This action was taken because some risks flow from the same deficiency in the system.

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

Table 4: DOEHRSDR 1.5.1 Vulnerability Matrix

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status
Medium Short-Term Risk	Win2K OS – Gold Disk	Finding: User rights and advanced user rights settings do not meet minimum requirements.	Too vague to correct. The TIO would like precise guidance for this vulnerability from JMISO.	Certification Team does NOT concur	MEDIUM Short-Term Risk

For Official Use Only

DOEHRSDR 1.5.1 Certification and Accreditation Report

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating>Status
Medium Residual Risk	Oracle Database	<p>Finding: The COTS Software has not been protected from modification.</p> <p>Impact: Trojan horses and other malicious code could be implanted in standard database executables that could corrupt database integrity or allow unauthorized access. Host systems should baseline their systems after application installation to collect data on application directories and files for future comparison in order to determine unauthorized modification.</p> <p>Recommendation: Establish and implement procedures to monitor any changes made to the database software.</p>	<p>Changes made to the database software are currently monitored manually. All changes made are captured in the Oracle audit tables and is available for review by DOEHRSDR DBAs. Further, the RTPO is pursuing the purchase of TripWire software. Upon completion of acquisition, TripWire will be implemented to monitor system changes in an automated manner.</p>	<p>The PO has a plan that manually monitors changes made to the database software. The PO has a plan to purchase and implement TripWire.</p> <p>The Certification Team will re-verify this finding within 90 days.</p>	LOW Residual Risk

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status		
Medium Residual Risk	Win2K OS – Gold Disk PDI ID#1806 FSO Checklist: 5.4.5.47NSA WIN2K Guide, Group Policy: Security Configuration Toolset Chap. 4, p. 41	<p>Finding: The Send download LanMan compatible password option is not set to "As Requested".</p> <p>Impact: The Local Area Network Manager (LanMan) is not compatible because there is a newer version that offers improved security. The version is NTLMv2. The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts from computers that are running Windows 2000. The Kerberos protocol is the protocol of choice in Windows 2000, when there is a choice. The Windows NTLM protocol was the default for authentication in Microsoft Windows NT version 4.0. It is retained in Windows 2000 for compatibility with clients and servers that are running Windows NT version 4.0 and earlier. It is also used to authenticate logons to stand-alone computers that are running Windows 2000.</p> <p>Recommendation: To configure the system to be protected, set the following key in the registry: LMCompatibilityLevel Value = 5.</p>	This finding is Not Applicable. There are no NT servers in the DOEHRSDR accreditation boundary. DOEHRSDR is implemented on an NT LAN by the TIO.	The PO is using the NT Domain authentication for ease of administering authorized users within the enclave. The NT Domain controller is outside this system's accreditation boundary and is a business function to assist administrators' access the system. Strong authentication of the administrators has been confirmed, and external access to the system is blocked by the enclave firewall.	However, DISA's recommendation to use the most stringent security possible is not being followed. The PO should strive to implement the recommended setting to improve overall security.	<p>Certification Team partially concurs</p> <p>Recommend that the risk be changed to LOW.</p>	LOW Residual Risk

DOEHRSDR 1.5.1 Certification and Accreditation Report

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status
Low	Oracle Database – Oracle DB SRR Results	<p>Finding: The ODBC tracing executable has not been removed from the host system.</p> <p>Impact: ODBC tracing may capture passwords or other sensitive information. Since ODBC tracing is used primarily to debug applications, it should not be required in a production environment.</p> <p>Recommendation: Remove the ODBC tracing executable from the system if it is feasible. The Microsoft ODBC trace executable is named Odbctrac.dll.</p>	The ODBC tracing utility is used by System Administrators to troubleshoot performance issues. Only System Administrators have access to this utility. System Administrators need access to this utility 24 hours as the system is operated both CONUS and OCONUS.	<p>Certification Team partially concurs</p> <p>Since the ODBC tracing utility is only used for troubleshooting and only available to System Administrators, the finding has been mitigated. However, the finding remains for documentation purposes.</p> <p>Finding remains LOW</p>	LOW Residual Risk

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status
LOW Residual Risk	Oracle Database – Oracle DB SRR Results	<p>Finding: Use of PKI authentication to access the database is not compatible with the DoD PKI implementation.</p> <p>Impact: Where possible, databases are encouraged to use Public Key Infrastructure (PKI) as the method of authentication in accordance with the Assistant Secretary of Defense (C3I) Memorandum, subject: "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DOD) Memorandum by ASD (C3I)," 17 May 2001.</p> <p>Recommendation: Configure database connections requiring use of PKI to comply with DoD PKI use requirements.</p>	<p>Currently, there is no clear DoD technical implementation guideline associated with PKI implementation at an application level. When clear guidance is provided, DOEHRs DR will implement this functionality.</p> <p>Although DoD policy related to PKI authentication is still vague, this finding will remain a risk until additional clarification is provided.</p> <p>Finding remains LOW</p>	<p>Certification Team partially concurs</p>	LOW Residual Risk

For Official Use Only**DOEHRs-DR 1.5.1 Certification and Accreditation Report**

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status
Low Residual Risk	DOD 8500.2 MAC II Sensitive IA Control COAS-2 CODP-2 COMS-2 COSP-1	<p>Finding: An alternate site has not been identified that permits the restoration of all mission or business essential functions as required by MAC II.</p> <p>Although a redundant server is established in a separate location at APG, a disastrous event may disable all DOEHRs-DR 1.5.1 capability with the loss of both servers. Previous Annual Review incorrectly indicated that redundant server had been moved off-site.</p> <p>Impact: MAC II requires that a system has the capacity to restore ALL mission or business function within 24 hours. Without an alternate site, DOEHRs-DR 1.5.1 cannot expect to meet this control requirement.</p> <p>Recommendation: Establish an alternate site for redundancy in a location adequately removed from the physical environment of APG.</p>	RTPO is in the process of determining an appropriate alternate site at a DISA location for DOEHRs-DR. Servers at APG are redundant in the event of failure.	Certification Team partially concurs DOEHRs-DR 1.5.1 should initiate plans to develop alternate site. Risk remains LOW until an alternate site becomes operational.	LOW Residual Risk

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating>Status
Low Short-Term Risk	DoD 8500.2 MAC II Sensitive IA Control ECPC-2	<p>Finding: DOEHRs-DR 1.5.1 programmer privileges to change production code and data are not limited and reviewed every 3 months.</p> <p>Impact: This is a specifically enhanced MAC II Control requirement to establish review of privileges on a short-term interval to further control and protect a MAC II system. The required MAC II protection is not implemented without compliance with ECPC-2.</p> <p>Recommendation: Develop and enforce a documented procedure to review privileges every 3 months, and adjust as appropriate.</p>	<p>09/10/04: RITPO has advised DOEHRs-DR 1.5.1 to review programmer privileges every three months in compliance with this MAC II IA Control.</p> <p>However, JMSO has insufficient time to re-validate this finding. JMSO recommends that DOEHRs-DR 1.5.1 incorporate this change in the SSAA. This risk will remain low until JMSO has the opportunity to review an amended SSAA to confirm RITPO representation.</p>	09/10/04: Certification Team concurs.	LOW Short-Term Risk

For Official Use Only

DOEHRSDR 1.5.1 Certification and Accreditation Report

Initial Risk Rating	System Area	Finding/Recommendations	Program Office Response/Mitigation Strategy	Certification Team's Response	Residual Risk Rating/Status
Low Short-Term Risk	DoD 8500.2 MAC II Sensitive IA Control DCPR-1 OMB A-130, App III	Finding: DOEHRSDR 1.5.1 CM Process does not enforce document updating. Most DOEHRSDR 1.5.1 SSA documents initially submitted for this C&A had not been revised in 3 years. Impact: Outdated documents delay or prohibit DITSCAP or Service CONs. Present inaccurate system descriptions; potential for business or security decisions to be made on inaccurate configuration descriptions. Recommendation: Develop and implement procedure to ensure documentation is reviewed and updated at least annually. Release Notes for all system changes are reported to CA at the earliest possibility.	This is inaccurate. DOEHRSDR DITSCAP documents are current and available for review.	Certification Team does not concur. The PO response does not address MAC II and OMB requirements that SSA documentation be kept updated to reflect present system configuration.	LOW Short-Term Risk

6 RISK ASSESSMENT SUMMARY

This Section summarizes the findings of the evaluation and presents the conclusions drawn regarding the extent of compliance with established DOD and MHS requirements. Recommendations for security control features, which will enable full compliance with security requirements and reduce security risks for the DOEHRS-DR 1.5.1 system, are also provided.

6.1 COMPLIANCE DETERMINATION CRITERIA

The following table summarizes the status of compliance with the reviewed SSAA documentation in support of an ATO.

Table 5: DOEHRS-DR 1.5.1 SSAA Documentation Compliance

Source(s) of Evaluation	Delivered	Compliance Status
System Security Authorization Agreement- 7/1/04	Yes	Compliant
System Security Concept of Operations- 8/13/04	Yes	Compliant
Information System Security Policy- 7/1/04	Yes	Compliant
Requirements Traceability Matrix – 6/30/04	Yes	Compliant
Security Design Document- 7/1/04	Yes	Compliant
Trusted Facility Manual- 7/1/04	Yes	Compliant
Configuration Management Plan- 7/1/04	Yes	Compliant
Certification Test & Evaluation(CT&E)Plan- 3/15/04	Yes	Compliant
Security Features User's Guide – 7/1/04	Yes	Compliant
System Rules of Behavior- 7/1/04	Yes	Compliant
Incident Response Plan- 7/1/04	Yes	Compliant
Contingency Plan- 8/23/04	Yes	Compliant
Personnel Security Controls- 7/1/04	Yes	Compliant
Memorandums of Agreement – (various dates)	Yes	Compliant
Security Awareness and Training Plan- 7/1/04	Yes	Compliant

DOEHRS-DR 1.5.1 Certification and Accreditation Report

6.2 EVALUATION RESULTS

With the closure of short-term risks, the DOEHRS-DR 1.5.1 system will meet the baseline security requirements of a MAC II Sensitive system. There are eleven (11) remaining vulnerabilities (1 Medium, and 10 Low). Four (4) risks are deemed short-term risks, and the remainder are considered residual risks

- The only medium risk can be closed by DOEHRS-DR 1.5.1 by adjusting user rights settings to meet minimum requirements
- One low risk can be closed by DOEHRS-DR 1.5.1 by minor amendments to the Change Management Process
- One low risk can be closed by DOEHRS-DR 1.5.1 by changing management procedures to include review of programmer privileges every three months, and update the SSAA to reflect this change.
- One low risk can be closed by DOEHRS-DR 1.5.1 by the establishment of an alternate site physically separated from APG in Aberdeen, Maryland

Following the closure of the Medium risk, the overall risk for DOEHRS-DR 1.5.1 is LOW.

6.3 CONCLUSIONS AND RECOMMENDATIONS

The Certification Team recommends to the Certifying Authority (CA) that DOEHRS-DR 1.5.1 be granted an Approval to Operate (ATO) by the DAA. It is further recommended that the DAA require compliance with the following general and special conditions:

1. General Conditions:
 - a. If the Resources Information Technology Program Office (RITPO) makes any changes to the configuration of DOEHRS-DR 1.5.1, the Program Office (PO) must assess and document the impact on the security policies and processes. This involves fully understanding any changes that are made to the security policies and processes, documenting any new vulnerability, conducting elimination or mitigation to reduce risk, and finally updating the System Security Authorization Agreement (SSAA) and supporting documents. The JMISO Certification Team must be notified, and provided a copy of the updated security documents.
 - b. The PO must use the following guidelines in determining the level of certification activities required when changes are made to the configuration of DOEHRS-DR 1.5.1, baseline:
 - 1) If the PO deems the changes to the configuration to be “minor”, the changes can be documented using Release Notes that have a security section. An example of a “minor” change would be the addition of functional changes that do not make any changes to the security policies and procedures.

DOEHRS-DR 1.5.1 Certification and Accreditation Report

- 2) If the PO deems the changes to the configuration to be more than “minor” but still less than a “major” change, a Risk Assessment must be coordinated with and validated by the JMISO Certification Team. The results normally will be documented as an addendum to the system accreditation report. An example of this type of change would be the addition of a new Commercial-Off-The-Shelf (COTS) product to the application or, adding one or more new interfaces to the system.
- 3) If the PO deems the changes to the configuration to be a “major” change, a full Certification and Accreditation effort that leads to a new Approval to Operate (ATO) will need to be performed by the JMISO Certification Team. Examples of “major” changes include changing the operating system, or changing a major component, such as the database used by the system.
 - c. Mitigation of the system’s technical risks, identified under “Specific Conditions” below, are not to be delayed for the duration of the approved certification, but rather completed by the PO as quickly as resources permit.

2. Specific Conditions:

It is recommended specifically that the following mitigation effort be continued to further reduce the risk to the DOEHRS-DR 1.5.1:

- Take all appropriate actions to close the Medium risk indicated in this report, or reduce this risk to a Low rating and to the extent that they may be considered an acceptable residual risk to the operation of DOEHRS-DR 1.5.1. The JMISO Certification Team and DOEHRS-DR 1.5.1 will coordinate efforts, prior to 01 December 2004, to allow JMISO verification that this task is completed by a review of amended SSAA documentation and procedures.
- Establish and document a procedure to ensure that the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA), including Appendices, is reviewed and updated as necessary upon any significant change to the system security or configuration and, at least, on an annual basis. DOEHRS-DR 1.5.1 will validate this action to the JMISO Certification Team prior to 01 December 2004
- Initiate efforts to establish an alternate site for DOEHRS-DR 1.5.1 at a location physically separate from APG in Aberdeen, Maryland

3. Other

Best practices and JMISO policy will require DOEHRS-DR 1.5.1 to resolve any relevant issues relating to the upcoming discontinuation of Microsoft support of Windows NT. Although not

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

considered a risk for the purposes of this Certification and Accreditation, these circumstances create a business risk because systems will be removed from Service networks if Windows NT is running and unsupported.

Further, the JMISO Certification Team recommends that the DAA require all of the above conditions to be satisfied as soon as possible and no later than the next Annual Review for DOEHRS-DR 1.5.1, unless completion dates otherwise are indicated.

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

**ATTACHMENT A
ACRONYMS**

For Official Use Only

ACRONYMS

Acronym	Description
AIS	Automated Information System
APG	Aberdeen Proving Ground
ATO	Approval to Operate
C&A	Certification and Accreditation
CA	Certifying Authority
CCB	Configuration Control Board
CHCS	Composite Health Care System
CHPPM	U.S. Army Center for Health Promotion and Preventive Medicine
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
CT&E	Certification Testing and Evaluation
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DBA	Database Administrator
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOEHRS	Defense Occupational and Environmental Health Readiness System
DOEHRS-DR	Defense Occupational and Environmental Health Readiness System – Data Repository
DOEHRS-HC	Defense Occupational and Environmental Health Readiness System – Hearing Conservation
DR	Data Repository
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Field Security Office
HC	Hearing Conservation

For Official Use Only

Acronym	Description
HTTPS	Hypertext Transfer Protocol-Secure
IA	Information Assurance
IATO	Interim Approval to Operate
IAVA	Information Assurance Vulnerability Alert
INFOCON	Information Operations Condition
INFOSEC	Information Systems Security
IP	Internet Protocol
ISS	Internet Security Systems
IT	Information Technology
JMISO	Joint Medical Information Systems Office
LAN	Local Area Network
MAC II	Mission Assurance Category II
MHS	Military Health System
MHz	Megahertz
MOA	Memorandums of Agreement
MS	Microsoft
MTF	Military Treatment Facility
NIPRNet	Unclassified But Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
OH	Occupational Health
OMB	Office of Management and Budget
OS	Operating System
PKI	Public Key Infrastructure
PMO	Program Management Office
PnP	Ports and Protocols
POC	Point-of-Contact
RITPO	Resources Information Technology Program Office
SA	System Administrator
SDD	Security Design Document
SFUG	Security Features User's Guide
SI	Sensitive Information
SLA	Security Level Agreements
SRR	Systems Readiness Review
SSAA	System Security Authorization Agreement
SSL	Secure Sockets Layer
SSP	System Security Policy

For Official Use Only

Acronym	Description
ST&E	Security Testing and Evaluation
STIG	Security Technical Implementation Guide
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TFM	Trusted Facility Manual
TIO	Technical Integration Office
TMA	TRICARE Management Activity
userid	User Identification
VCTS	Vulnerability Compliance Tracking System
VMS	Vulnerability Management System
VPN	Virtual Private Network

For Official Use Only

**ATTACHMENT B
SECURITY REQUIREMENTS AND/OR REQUIREMENTS
TRACEABILITY MATRIX**

For Official Use Only

SECURITY REQUIREMENTS AND/OR REQUIREMENTS TRACEABILITY MATRIX

Introduction

This section contains the Security Requirements Traceability Matrices used by DOEHRS-DR 1.5.1, which is incorporated in the SSAA as Appendix F. Requirements Traceability Matrix (RTM)

DoD 8510.1-M, requires that directives and security requisites be analyzed to determine the system security requirements. Sections of directives are parsed into basic security requirement statements. The security requirements are entered into a RTM or RTMs to support the Certification and Accreditation (C&A) effort.

DEFENSE OCCUPATIONAL ENVIRONMENTAL HEALTH READINESS
DATA REPOSITORY (DOEHRs-DR 1.5.1)
SECURITY REQUIREMENTS TRACEABILITY MATRIX

DoD unclassified directives and security requisites were extracted from the Defense Information Systems Agency (DISA) Requirements Traceability Matrix and analyzed to determine the applicable system unclassified security requirements. All rescinded DoD directives and regulations were removed, some MHS requirements (except DoDI 8200.2 entries) added, and the table entries renumbered. The DoDI 8500.2 RTM follows this table.

(The review column identifies the review process for each requirement. I = Interview, D = Document review, T = Test, and O = Observation.)

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
GENERAL REQUIREMENTS (GEN)								
GEN.1	Agencies shall implement and maintain a program to assure that adequate security (Appendix III, <i>Security of Federal Automated Information Resources</i> , A. Requirements, 3. Automated Information Security Program) is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.	OMB A-130, Appendix III (A. 3).				X		MET - DITSCAP Process and Annual Reviews

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	B	T	O	
GEN.2	Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards and procedures issued by the Office of Management and Budget, Department of Commerce, General Services Administration, and Office of Personnel Management.	OMB A-130, Appendix III (A.3).		X				MET – SSAA and Appendices
GEN.3	Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives.	OMB A-130, Appendix III (A.3).		X	X			N/A – No national security data processed or maintained
GEN.4	Ensure that cost effective security products and technical products are appropriately used within the system.	OMB A-130, Appendix III (A.3.a.2.f).		X	X	X		MET
GEN.5	Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.	OMB A-130, Appendix III (A.3.b.2.f).						MET – On site testing at CHPPM
TECHNICAL (TEC)								
TEC.1	Ensure that cost effective security products and technical products are appropriately used within the system.	OMB A-130, Appendix III (A.3.a.2.f).			X	X	X	MET
TEC.2	Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.	OMB A-130, Appendix III (A.3.b.2.f).					X	MET – On site testing at CHPPM. User Permissions

Req. No.	Requirement	Source	Related Requirement	Review					Comments
				I	D	T	O		
DISCRETIONARY ACCESS CONTROL (DAC)									
DAC.1	The TCB shall define ... access between named users and named objects (for example, files and programs) in the ADP system.	OMB Circ. A-123 II.			X				MET - Access permissions
DAC.2	The TCB shall ... and control access between named users and named objects (for example, files and programs) in the ADP system.	OMB Circ. A-123 II.			X				MET - Requests reviewed/approved by working group; implemented by S/A
DAC.3	The enforcement mechanism (for example, self/group/public controls, access controls lists) shall allow users to specify ... sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.	OMB Circ. A-123 II.				X			MET - On site testing at CHPPM
DAC.4	[The enforcement mechanism (for example, self/group/public controls, access controls lists) shall allow users to ...control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.	OMB Circ. A-123 II.				X			MET - On site testing at CHPPM
DAC.5	The DAC mechanism shall, either by explicit user action or default, provide that objects are protected from unauthorized access.	OMB Circ. A-123 II.				X			MET - Access on need to know; reviewed by system
DAC.6	Access permission to an object by users not already permitted access shall only be assigned by authorized users.	OMB Circ. A-123 II.				X			MET - S/A or DBA ; approval by working group
ACCOUNTABILITY (ACO)									

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments	
				I	D	T	O		
ACO.1	There shall be in place safeguard to ensure each person having access to an AIS may be held accountable for his or her actions on the AIS. There shall be an audit trail providing a documented history of DAIS use. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.	OMB Circ. A-123 II.				X		MET – On site testing at CHPPM	
AUDIT (AUD)									
AUD.1	The audit trial shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.	NIST 800-18 (6.MA.4, 6.GSS.3).				X		MET – On site testing at CHPPM	
AUD.2	For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event.	NIST 800-18 (6.MA.4, 6.GSS.3).				X		MET – On site testing at CHPPM	
SYSTEM INTEGRITY (SI)									

September 2004

B-5

DOEHRSS-DR I.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
SI.1	Virus prevention measures commensurate with the level of risk identified in the risk analysis shall be employed to ensure the integrity of the software.	MHS AIS SPM (5.8.3), NIST 800-18 (5.MA.6, 5.GSS.6).		X	X			MET – Addressed in SSAA. However, DOEHRSS DR is hosted at CHPPM and is protected by the enclave boundary defense implemented by CHPPM. This requirement is a site accreditation issue
SECURITY TESTING (TST)								
TST.1	The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms functional testing. Where practical, individuals who conduct the certification will be independent of the system's developers. FIPS PUB 102 provides guidance for certification testing.		DoDI 5200.40 (E3.5.2.1).				X	N/A- System in operational/deployment phase. PO supplied ST&E Plan. Certification testing with this DITSCAP
TST.2	The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation.		DoDI 5200.40 (E3.5.2.1.1).				X	MET - This C&A
TST.3	Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB.		DoDI 5200.40 (E3.5.2.1.1).				X	MET – On site testing at CHPPM
MANAGEMENT AND PROCEDURAL								

September 2004

B-6

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments	
				I	D	T	O		
M&P.1	Management controls must provide reasonable assurance against waste, loss, unauthorized use, and misappropriation.	OMB Circ. A-123 II.		X	X			MET	
M&P.2	Accountability for the custody and use of resources should be assigned and maintained.	OMB Circ. A-123 II.		X				MET – IASO responsibility	
M&P.3	At a minimum agency (security) programs shall include the following controls: Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.	OMB A-130, Appendix III (A. 3.a.1).		X	X			MET – IASO responsibility	
M&P.4	At a minimum agency (security) programs shall include the following controls:... Ensure that management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system.	OMB A-130, Appendix III (A.3.b.1).		X				MET – IASO responsibility for this application	
M&P.5	ADP personnel shall notify the system manager and the ADP manager whenever unauthorized personnel seek access to system information.	DoD 5400.11-R App A (2c).		X				MET - Audit function; training; ROB	
M&P.6	Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.	DoD 5400.11 (E.2.h). DoD 5400.11-R (App. A, B.1)		X				MET – SSL transmission client to server	

DOEHRSDR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
M&P.7	There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.	DoD 5400.11-R (App. A, B.1), DoD 5200.1-R (6-603 d.).		X			MET
RISK ANALYSIS (RA)							
RA.1	Risks will be generally assessed and actions taken to manage them.	OMB A-130, Appendix III (B. Descriptive Information, third indented paragraph).		X			MET – DITSCAP; and Annual Reviews; periodic testing throughout Life Cycle
RA.2	A formal risk assessment must be conducted for AISSs that process unclassified personal information to safeguard against the likelihood of compromise or threats to the information contained within the installation.	DoD 5400.11-R, App. A (para. H).		X			MET – C&A and Annual Reviews
SECURITY PLAN (SP)							
SP.1	System Security Plan—Plan for adequate security of each general support system as part of the information resource management (IRM) planning process. The security plan shall be consistent with guidance issued by NIST.	OMB A-130, App. III [A.3.a.(2)].		X			N/A – This is an application; type accreditation

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
SP.2	Application Security Plan—Plan for adequate security of each major application, taking into account the security of all systems in which the application will operate. The security plan shall be consistent with guidance issued by NIST.	OMB A-130, App III (A.3.b.2).		X			MET – SSAA and Appendices
SP.3	Executable software authorized to run on a computer system shall be identified in that system's security plan.	NIST 800-18 (5.MA.5, 5.GSS.5).		X			MET – In SSAA and Appendices
SP.4	Application Security Plan—A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S. C. Chapter 35) and Section 8(b) of this circular (OMB Circular A-130).	OMB A-130, Appendix III [A. 3. a. (2)], 8 February 1996	44 U.S. C. Chapter 35	X	X		N/A – MHS responsibility; PO cooperation
SP.5	System Security Plan—A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S. C. Chapter 35).	OMB A-130, App III (A.3.b.2).	44 U.S. C. Chapter 35	X			N/A – MHS responsibility; PO cooperation
ACCREDITATION (ACR)							
ACR.1	Each AIS shall be accredited to operated in accordance with a DAA-approved set of security safeguards.	OMB A-130, App III (A.3.a.4, b.4), NCSC-TG-031& 032.			X		MET – Prior ATO and Annual Review

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
ACR.2	Ensure that a management official authorizes in writing the use of each general support system and major application based on implementation of its security plan before beginning or significantly changing processing in the system.	OMB A-130, App III (A.3.a.4, A.3.b.4).	NCSC-TG-032, NIST 800-18 (Exec Summary)	X				MET – Prior ATO
ACR.3	Use of the system shall be re-authorized at least every three years.	OMB A-130, App III (A.3.a.3, A.3.b.3).	NCSC-TG-031 &032, NIST 800-18 (Exec Summary)	X				MET – This ATO is a re-accreditation
ACR.4	A schedule to accomplish the accreditation is developed and implemented.	DoDI 5200.40 (E3.1.3).		X				MET – Process completely described; unable to determine actual dates prior to events
REVIEW AND REVISION REQUIREMENTS (R&R)								
R&R.1	Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.	OMB A-130, App III (A.3.a.3, A.3.b.3).			X			MET – 3 yr. DITSCAP C&A; Annual Reviews

DOE/HRS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
R&R.2	Security plans shall be reviewed and revised when major changes to the system occur or three years have elapsed since the date of certification.	OMB A-130, APP III.	NIST 800-18 (Exec Summary)	X				PARTIALLY MET – SSA needs updating with all substantial changes to application. Release Notes should to be sent to JMISO. DITSCAP documents presented to JMISO for this C&A were completely outdated
Risk: LOW								
RULES OF THE SYSTEM (RS)								
RS.1	Rules of the System—Establish a set of rules of behavior concerning the use of, security in, and the acceptable level of risk for the system. The rules shall be based on the needs of the various users of the system.	OMB A-130, App III (A.3.a.2.a), 8 February 1996.	DoD 5400.11 (E.2.i), NIST 800-18 (4.3).		X			MET – Rules of Behavior (ROB) in SSA
RS.2	Application Rules—Establish a set of rules concerning use of and behavior within the application.	OMB A-130, App III (A.3.b.2.a).			X			MET – ROB specifically written by application

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
RS.3	Establish rules of conduct for DoD personnel involved in the design, development, operation, or maintenance of any system of records and train them in these rules of conduct.	DoD 5400.11 (E.2.i).		X				MET – ROB and required training
RS.4	The (Rules of the System and Application Rules) shall be as stringent as necessary to provide adequate security for the application and the information in it.	OMB A-130, App III (A.2.a.2.a) and (A.3.b.2.a).	NIST 800-18 (4.3).	X				MET
RS.5	Such rules of the system shall clearly delineate responsibilities and expected behavior of all individuals with access to the system... (and) shall be clear about the consequences of behavior not consistent with the rules.	OMB A-130, App III (A.3.a.2, A.3.b.2.a)	NIST 800-18 (4.3).	X				MET
RS.6	Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.	OMB A-130, App III (A.3.a.2.b, A.3.b.2.b).	DoD 5400.11 (E.2.i).	X	X			MET
RS.7	(The rules of the system) shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities.	OMB A-130, App III (A.3.a.2, A.3.b.2.a)	NIST 800-18 (4.3).	X	X			MET – All data in this system has same priority. DOEHRs DR relies on CHPPM for restoration activity. This requirement is a site accreditation issue

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
DOCUMENTATION (DOC)							
DOC.1	A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact.	OMB A-130, App III (A.3.a.2, A.3.b.2)a).		X			MET - SFUG
DOC.2	A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a security facility.	OMB A-130, App III (A.3.a.2, A.3.b.2.a).		X			MET - TFM
DOC.3	The procedures for examining and maintaining audit files as well as the detailed audit record structure for each type of audit event shall be given.	OMB A-130, App III (A.3.a.2, A.3.b.2)a).		X	X		MET – However, the system relies on CHPPM for backup activity. This requirement is a site accreditation issue
ACCESS CONTROL (ACC)							
ACC.1	Access to resources and records should be limited to authorized individuals...	OMB Circ. A-123 II.		X			MET – Issued UserID and password required; DAC
PASSWORD CONTROL (PC)							
PC.1	Passwords shall be protected to the same degree as the information to which they provide access.	MHS AIS Policy.			X		MET – On site testing at CHPPM

September 2004

B-13

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments	
				I	D	T	O	
PC.2	Passwords shall not be shared.	MHS AIS Policy.		X				MET - ROB
PC.3	The method of password distribution will be appropriate to the level of information they protect.	CSC-STD-002-85.	MHS AIS Policy.		X			MET – On site testing at CHPPM
PC.4	Each user will have a unique user identification and password. Password usage shall meet the standards set forth in FIPS PUB 112.	CSC-STD-002-85.			X			MET
DISPOSITION OF COMPUTER SYSTEM MEDIA (MD)								
MD.1	Computer system media containing sensitive information must be protected and marked as For Official Use Only	DoD 5200.1-R (2-200 b., 6-601.)	DoD 5400.11-R (App. A, C.2), DoD 5400.7-R (4-100, 4-200 a.)	X	X	X		MET
MD.2	Magnetic floppy disks containing sensitive information should be sanitized using an approved overwrite program or process. A degausser may be used in place of overwriting.	DoD 5400.11-R (App. A, G.1).		X				N/A – DOEHRS DR does not utilize or maintain floppy discs
CONTINGENCY PLANS (CP)								
CP.1	Contingency plans must be developed to ensure that AIS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service.	OMB A-130, App III (A.3.a.2, A.3.b.2)e).			X			MET - COOP in SSAA

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
CP.2	Contingency plans shall be periodically tested.	OMB A-130, App III (A.3.a.2, A.3.b.2)e).			X			MET by documentation – However, testing conducted by CHPPM @ Aberdeen. This requirement is a site accreditation issue
CP.3	Rules of the system shall define service provision and restoration priorities.	OMB A-130, App III (A.3.a.2, A.3.b.2)a).	NIST 800-18 (4.3).	X	X			MET – However, the system relies on CHPPM for priority determination. This requirement is a site accreditation issue
INCIDENT RESPONSE CAPABILITY (IR)								
IR.1	Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.	OMB A-130, App III (A.3.a.2, A.3.b.2).d).	NIST 800-18 (5.GSS.9).		X			MET – IRP in SSAA. Help desk availability
IR.2	This (incident response) capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with DoD guidance.	OMB A-130, App. III (A.3.a.2, A.3.b.2)f.	NIST 800-18 (5.GSS.9).		X			MET – IRP in SSAA. However, DOEHRS DR relies on CHPPM for IRP execution. This requirement is a site accreditation issue

September 2004

B-15

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
GENERAL (PHS)							
PHS.1	AIS hardware, software, and documentation, and all sensitive unclassified data handled by the AIS shall be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification (that is, data integrity shall be maintained).	DoD 5400.11-R (App. A, D.2).		X			MET
PHS.2	Physical safeguards must be established to ensure records in every system of records are protected from identified threats that could result in unauthorized access or alteration.	DoD 5400.11-R App. A (D.1).	DoD 5200.1-R (2-203).	X			MET by documentation – However, PHYSEC contracted to CHPPM @ Aberdeen. This requirement is a site accreditation issue
MARKINGS (MAR)							
MAR.1	Sensitive unclassified output shall be marked to accurately reflect the sensitivity of the information.	DoD 5200.1-R (2-203, 6-601).	DoD 5400.7-R (4-100), DoD 5400.11-R (App. A.C.2).	X	X		MET – FOUO; no hard media output
MAR.2	Safeguards must be established to ensure that records in every system of records that contains personal information are marked and protected as at least “For Official Use Only.”	DoD 5400.11-R (App. A. C.2).	DoD 5200.1-R (2-203, 6-601), DoD 5400.7-R (4-100).	X	X	X	MET
CLEARANCES (PS)							

September 2004

B-16

DOEHRSDR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments		
				I	D	T	O		
PS.1	Personnel accessing computer systems shall have clearances commensurate with the highest level of information processed by the systems.	OMB A-130, App III (A.3.a.2, A.3.b.2)c).			X			MET – ADP II clearances required	
PS.2	All military, government civilian, consultants, and contractors who design, develop, operate, or maintain an AIS shall possess appropriate clearances and authorizations for access to system components, output, or documentation. Automated data processing (ADP) position categories shall be assigned and documented for all personnel with access to AISs.	DoD 5200.2-R (3-614).			X			MET – ADP II clearances required	
PS.3	Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of the harm they could cause.	OMB A-130, App III (A.3.a.2, A.3.b.2)c).			X	X		MET	
PS.4	Such screening (of individuals authorized to bypass security controls) shall occur prior to an individual being authorized to bypass controls and periodically thereafter.	OMB A-130, App III (A.3.a.2, A.3.b.2.c).			X	X		MET	
SECURITY TRAINING (TR)									
TR.1	There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS.	OMB A-130 App. III A.3.a.2)b).					X	MET – Read and acknowledge prior to first access	

September 2004

B-17

DOE/HRS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments	
				I	D	T	O	
TR.2	Computer system security training is required for all persons involved in the management, use, or operation of systems which process sensitive information.	OMB A-130, App III (A.3.a.2.b, A.3.b.2.b).	DoD 5400.11-R App. A (C-7), NIST 800-18 (5.MA.8, 5.GSS.8).		X			MET – Read and acknowledge prior to first access
TR.3	The program shall ensure that all persons responsible for the AIS and/or information, therein, and all persons who access the AIS are aware of proper operational and security- related procedures and risks.	OMB A-130, App III (A.3.a.2.b. A.3.b.2.b).			X			MET – Read and acknowledge prior to first access
TR.4	Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.	OMB A-130, App III (A.3.a.2.b, A.3.b.2.b).	NIST 800-18 (5.MA.8, 5.GSS.8).		X			MET – Read and acknowledge prior to first access
TR.5	Such (security) training shall assure that employees are versed in the rules of the system [adopted pursuant to OMB A-130], be consistent with NIST & OPM guidance & and apprise them of available assistance, security products & techniques.	OMB A-130, App III (A.3.a.2.b, A.3.b.2.b).	NIST 800-18 (5.MA.8, 5.GSS.8).		X			MET by documentation – However, system relies upon CHPPM/MTFs/Clinics for training. This is also a site accreditation issue
TR.6	New employees responsible for the management, use, or operation of computer systems that process sensitive information shall receive computer security training meeting the requirements of 5 CFR, Pt 930, within 60 days of their appointment.	OMB A-130, App III (A.3.a.2.b, A.3.b.2.b).			X			MET – Read and acknowledge prior to first access

September 2004

B-18

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
TR.7	Continuing training is required for persons whenever there is a significant change in the information security environment or procedures, or when they enter a new position which deals with sensitive information.	OMB A-130 App III.	NIST 800-18 (5.MA.8, 5.GSS.8).				MET by documentation – However, system relies upon CHPPM, MTFs or Clinics for training. This is also a site accreditation issue
TR.8	Periodic refresher training is required for persons involved in the management/use/operation of computer systems which process sensitive information. The frequency of refresher training shall be based on sensitivity of information processed.	OMB A-130.	NIST 800-18 (5.MA.8, 5.GSS.8).		X		MET – Annual refresher required of all users
TR.9	A record of security training which includes the following shall be maintained by the Component: a. The name of the person briefed, b. The content of the briefing, c. The date of the briefing.	OMB A-130 App III.			X		MET – Acknowledgement required at each training
SENSITIVE INFORMATION COMSEC REQUIREMENTS (SIC)							
SIC.1	If a risk analysis indicates additional security measures (encryption) are necessary, the following are some of the options available:		DoD C-5200.5 (D.4).		X	X	X
SIC.2	a. Products which conform to the Data Encryption Standard in FIPS PUB 46-1 and FIPS PUB 140-1 or their successors.		DoD C-5200.5 (D.4).		X	X	X

September 2004

B-19

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments	
				I	D	T	O	
SIC.3	Encryption, using equipment and keying' material approved by the NSA for the transmission of classified information (Type 1 products).	DoD C-5200.5 (D.4).		X	X	X	X	N/A – However, there may be future HIPAA implications.
SYSTEM INTERCONNECTION (SIT)								
SIT.1	Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.	OMB A-130, App III (A.3.a.2.g., A.3.b.2.g.).			X			MET – Addressed in SSAA
SIT.2	Where connection (with other systems) is authorized, controls shall be established which are consistent with the rules of the system and accordance with guidance from NIST.	OMB A-130, App III (A.3.a.2.g., A.3.b.2.g.).			X			MET – Addressed in SSAA
ENCLAVE BOUNDARY DEFENSE (EBD)								
EBD.1	Intrusion Detection—Certify and evaluate the availability and effectiveness of tools and procedures to ensure real-time monitoring and alerts, intrusion detection, network analysis, audit analysis, user management, risk analysis, and network configuration management tools.	DoD 8510.1-M, JUL00.			X			MET – DOEHRS relies upon CHPPM @ Aberdeen for IDS. This requirement is a site accreditation issue
VULNERABILITY AND INCIDENT MANAGEMENT (VIM)								

DOEHRS-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments		
				I	D	T	O		
VIM.1	Assurance—Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy.	DoD 5200.40, Dec 97 and DoD 8510.1-M, Jul 00.		X			X	MET – DITSCAP C&A process	
VIM.2	Interim Approval To Operate (IATO)—Information system may be granted and Interim Approval To Operate (IATO) in accordance with a DAA-approved set of security safeguards. The IATO will allow the information system to deploy while enhancement to the security posture of the information system are being implemented	DoD 5200.40, Dec 97 and DoD 8510.1-M, Jul 00.		X			X	N/A – This is an ATO certification.	
VIM.3	Approval to Operate (ATO)—Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy.	DoD 5200.40, Dec 97 and DoD 8510.1-M, Jul 00.		X			X	MET – DITSCAP C&A process	
VIM.4	System Security Periodic Reviews—Information system shall be subject to system security periodic reviews to ensure no new security risk to the information system has been introduced since the receipt of an ATO for the information system. The periodic reviews will also validate that any changes to the information system since the receipt of an ATO are properly documented.	DoD 5200.40, Dec 97 and DoD 8510.1-M, Jul 00.		X				MET – Annual Review by MHS IA in 2003	

DOEHRs-DR 1.5.1 Certification and Accreditation Report

Req. No.	Requirement	Source	Related Requirement	Review			Comments
				I	D	T	
VIM.5	Re-Accreditation—Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy.	DoD 5200.40, Dec 97 and DoD 8510.1-M, Jul 00.		X		X	MET – This C&A is a re-accreditation

September 2004

B-22

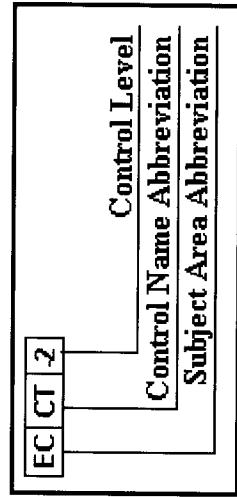
DODI 8500.2, MAC II SENSITIVE UNCLASSIFIED IA CONTROLS REQUIREMENTS TRACEABILITY MATRIX

To support the certification and accreditation (C&A) effort, the following Requirements Traceability Matrix (RTM) table was developed using DoDI 8500.2 sensitive unclassified Mission Assurance Category (MAC) II Information Assurance (IA) controls. (The review column identifies the review process for each requirement. I = Interview, D = Document review, T = Test, O = Observation, NA = Not Applicable)

IA Control Subject Areas Legend:

Abbreviation	Subject Area Name
DC	Security Design & Configuration
IA	Identification and Authentication
EC	Enclave and Computing Environment
EB	Enclave Boundary Defense
PE	Physical and Environmental
PR	Personnel
CO	Continuity
VI	Vulnerability and Incident Management

Elements of an IA Control Number:



IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Continuity									
Availability	COAS-2	Alternate Site Designation	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	An alternate site is identified that permits the restoration of all mission or business essential functions.				X	NOT MET – No alternate site is identified, although redundant server hosted at Aberdeen in separate building

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Test	Review				Comment
					I	D	T	O	
Availability	COBR-1	Protection of Backup and Restoration Assets	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.	X	X			Risk: LOW
Availability	CODB-2	Data Back-up Procedures	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.		X			MET – On site testing at CHPPM
Availability	CODP-2	Disaster and Recovery Planning	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)	X	X			PARTIALLY MET – COOP in SSAA. However, CHPPM is tasked with the implementation of the plan. No alternate site; cannot determine that total resumption is realistic if the redundant servers are destroyed in a single event. Previous ATO recommended redundant server be moved off-site

September 2004

B-25

For Official Use Only

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Availability	COEB-1	Enclave Boundary Defense	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Enclave boundary defense at the alternate site provides security measures equivalent to the primary site					Risk: LOW
Availability	COED-1	Scheduled Exercises and Drills	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The continuity of operations or disaster recovery plans are exercised annually.	X	X			MET – Contracted to CHPPM @ Aberdeen. DOEHRSS DR relies on the site for testing of the COOP. COOP included in SSAA; PO unable to provide specifics or lessons learned from last testing necessary to update COOP
Availability	COEF-2	Identification of Essential Functions	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Mission and business essential functions are identified for priority restoration planning along with all assets supporting mission or business essential functions (e.g., computer-based services, data and applications, communications, physical infrastructure).					X MET – Functions deemed to be same priority; COOP in SSAA; execution of recovery procedures to be conducted by CHPPM @ Aberdeen
Availability	COMS-2	Maintenance Support	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Maintenance support for key IT assets is available to respond 24 X 7 immediately upon failure.					PARTIALLY MET – Maintenance addressed in SSAA; Procedures implemented by CHPPM @ Aberdeen. Without an alternate site,

September 2004

B-26

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
									guarantee of full restoration of service in 24 hrs through maintenance is impossible. This control is a site accreditation issue, but cannot be resolved without an alternate hot or warm site. Risk merged with CODP-2
Availability	COPS-2	Power Supply	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators.	X	X			MET by documentation - Contracted to CHPPM @ Aberdeen. COOP included in SSAA. This control is a site accreditation issue.
Availability	COSP-1	Spares and Parts	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.	X	X			PARTIALLY MET- Maintenance addressed in SSAA; Procedures implemented by CHPPM @ Aberdeen. Without an alternate site, guarantee of full restoration of service in 24 hrs through availability of spares is impossible. This control is a site accreditation issue, but cannot be resolved without an alternate hot or warm site. Risk merged with

September 2004

B-27

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
									CODP-2
Availability	COSW-1	Backup Copies of Critical SW	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.	X	X			MET – At least one copy maintained at RITPO CM library; not collocated
Availability	COTR-1	Trusted Recovery	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.	X	X			MET– COOP included in SSAA; Procedures implemented by CHPPM @ Aberdeen. This control is a site accreditation issue
Identification and Authentication									
Integrity	IAKM-2	Key Management	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.	X	X			MET – However, security tokens not yet required in DoD for this system
Integrity	IATS-2	Token and Certificate Standards	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificates and hardware security token (when available) or an NSA-certified product.			X		MET –Server PKI, but tokens not a requirement for this system

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Enclave and Computing Environment									
Confidentiality	ECAD-1	Affiliation Display	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two-character country code in: - DoD user e-mail addresses (e.g., <u>john.smith ctr@army.mil</u> or <u>john.smith.uk@army.mil</u>); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command).	X			X	N/A
Confidentiality	ECAN-1	Access for Need-to-Know	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced				X	MET – Unique Userid and password required. I&A issued only after DOEHRS working group approval on need to know basis and clearance determination;

September 2004

B-29

DOE/HRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
				for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access: (1) Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction. (2) Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction. (3) Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions.					implemented by SA or DBA
Confidentiality	ECAR-2	Audit Record Content		DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.					MET – On site testing at CHPPM

September 2004

B-30

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Test	Review					Comment
					I	D	T	O	N	
				terminal or access port and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system.						
Integrity	ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.	N A	N A	N A	N A	N A	When an IA Control is required for both integrity and confidentiality, the higher level prevails (DoDI 8500.2, E4.1.5). See ECAT-2.
Integrity	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.	X					MET – DOEHRS relies upon CHPPM for immediate alert. This control is a site accreditation issue
Integrity	ECCD-2	Changes to Data	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.					X	MET – On site testing at CHPPM

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Confidentiality	ECCR-1	Encryption for Confidentiality (Data at Rest)	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.				X	N/A – Static encryption not required by information owner
Confidentiality	ECCT-1	Encryption for Confidentiality (Data in Transit)	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).		X			MET – SSL for all sensitive information
Integrity	ECDC-1	Data Change Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.		X			MET – Backup system in place. Daily backup
Confidentiality	ECIC-1	Interconnections among DoD Systems and Enclaves	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance.		X		X	N/A – No interconnections or external interfaces. Internal interface with DOEHRSS HC.
Integrity	ECID-1	Host Based IDS	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain		X	X		MET – DOEHRSS DR relies upon CHPPM @ Aberdeen hosting enclave for PHYSEC,

September 2004

B-32

For Official Use Only

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Integrity	ECIM-1	Instant Messaging	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	name servers (DNS).					including IDS This control is a site accreditation issue
Confidentiality	ECLC-1	Logon	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DOD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.	X			X	N/A – No IM in DOEHRSS DR
Confidentiality	ECLP-1	Least Privilege	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Successive logon attempts are controlled using one or more of the following: - access is denied after multiple unsuccessful logon attempts. - the number of access attempts in a given period is limited. - a time-delay control system is employed. If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions.		X			MET – On site testing at CHPPM
								X	MET – On site testing at CHPPM

September 2004

B-33

For Official Use Only

DOEHRs-DR I.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
				privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.					
Confidentiality	ECML-1	Marking and Labeling	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.	X	X			MET - FOUO
Confidentiality	ECMT-1	Conformance Monitoring and Testing	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.				X	MET – On site testing at CHPPM
Integrity	ECND-2	Network Device	DoDI 8500.2, 6	An effective network device control	X	X			MET – System relies on

September 2004

B-34

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
		Controls	Feb 03, Encl. 4, Attach. 2.	program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions, e.g., IA VA. Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.					CHPPM @ Aberdeen for hardware and PHYSIC equipment, testing and procedures. This control is a site accreditation issue
Confidentiality	ECNK-1	Encryption for Need-To-Know	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality).	X	X			X N/A – All DOEHRs DR data at same classification level
Integrity	ECPA-1	Privileged Account Control	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments.				X	MET – On site testing at CHPPM
Integrity	ECPC-2	Production Code	DoDI 8500.2, 6	Application programmer privileges to				X	NOT MET – Not

September 2004

B-35

For Official Use Only

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Test	Review				Comment
					I	D	T	O	
Confidentiality	ECRC-1	Resource Control	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object.	X	X			N/A – After Logon and Logoff, new session is initiated; residual data deleted
Integrity	ECRG-1	Audit Reduction and Report Generation	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Tools are available for the review of audit records and for report generation from audit records			X		MET – On site testing at CHPPM
Integrity	ECRR-1	Audit Record Retention	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.		X	X		MET – No SAMI. Audit records are indefinite, and exceed one year
Availability	ECSC-1	Security Configuration Compliance	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.		X			MET
Integrity	ECSD-2	Software Development Change	DoDI 8500.2, 6 Feb 03, Encl. 4,	Change controls for software development are in place to prevent		X			MET – RITPO has a Chartered CCB and

September 2004

B-36

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
		Controls	Attach. 2.	unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.						CMMMP process. No changes since DOEHRSS DR migrated to RITPO
Integrity	ECTB-1	Audit Trail Backup	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The audit records are backed up not less than weekly onto a different system or media than the system being audited.		X				MET – On site testing at CHPPM
Confidentiality	ECTC-1	Tempest Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.					X	N/A – TEMPEST not required
Integrity	ECTM-2	Transmission Integrity Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).		X				MET – On site testing at CHPPM

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Integrity	ECTP-1	Audit Trail Protection	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The contents of audit trails are protected against unauthorized access, modification or deletion.		X			MET – On site testing at CHPPM
Availability	ECVI-1	Voice over IP	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.	X				N/A – No VoIP in the application
Availability	ECVP-1	Virus Protection	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.					MET – Virus protection addressed in SSAA; However, DOEHS DR relies upon MTFs and CHPPM @ Aberdeen to implement such protection. This control is a site accreditation issue
Confidentiality	ECWM-1	Warning Message	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to			X	X	MET – Warning banners are displayed at logon

September 2004

B-38

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				
					I	D	T	O	N
Availability	ECWN-1	Wireless Computing and Networking	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings, or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.		X		X	N/A- On site testing at CHPPM confirms no wireless
Confidentiality	IAAC-1	Account Control	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	X	X			MET - Access on Need-to-Know ; determined by DOEHRS DR; accounts established based on determination
Enclave Boundary Defense									
Confidentiality	EBBD-2	Boundary Defense	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in	X	X			MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen and MTFs for boundary defense. This

September 2004

B-39

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
				the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.					control is a site accreditation issue
Availability	EBCR-1	Connection Rules	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The DoD information system is compliant with established DoD connection rules and approval processes.	X	X			MET by documentation – System relies on CHPPM for connection rules. This control is a site accreditation issue
Confidentiality	EPPW-1	Public WAN Connection	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ).	X	X			MET – DMZ at CHPPM
Confidentiality	EBRP-1	Remote Access for Privileged Functions	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures, such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/IAO reviews the log for every remote session.	X	X			MET – Only system administrator has remote access. VPN implemented. Recorded in audit trail
Confidentiality	EBRU-1	Remote Access for User Functions	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access				X	MET – On site testing at CHPPM

September 2004

B-40

For Official Use Only

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Test	Review				Comment
					I	D	T	O	
				always uses encryption to protect the confidentiality of the session. The session level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.					
Availability	EBV/C-1	VPN Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	All VPN traffic is visible to network intrusion detection systems (IDS).			X		MET – On site testing at CHPPM
Identification and Authentication									
Confidentiality	IAGA-1	Group Identification and Authentication	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA).			X		MET – On site testing at CHPPM
Confidentiality	IAIA-1	Individual Identification and Authentication	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters,			X		MET – On site testing at CHPPM

September 2004

B-41

DOEHRSS-DR 1.5.1 Certification and Accreditation Report

IA Service #	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
				lower case letters, numbers, and special characters, including at least one of each (e.g., empAgd2). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.					
Personnel									
Confidentiality									
	PRAS-1	Access to Information		DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Individuals requiring access to sensitive information are processed for access authorization in accordance with DOD personnel security policies.	X			MET – All users must have required ADP II clearance

September 2004

B-42

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Confidentiality	PRMMP-1	Maintenance Personnel	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented.		X			MET – Maintenance personnel ADP II clearances
Confidentiality	PRNPK-1	Access to Need-to-Know Information	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.		X			MET – Access requires approval of working group, and implementation by SA or DBA
Availability	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.		X			MET – ROP in the SSAA
Integrity	PRTN-1	Information Assurance Training	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans		X			MET – Training prior to access, and each year thereafter; training must be acknowledged by user. However, DOEHRS DR relies upon CHPPM or sites to

September 2004

B-43

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
Physical and Environmental									
Confidentiality	PECF-1	Access to Computing Facilities	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.				X	MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen and MTFs for boundary defense. This control is a site accreditation issue
Confidentiality	PECS-1	Clearing and Sanitizing	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C31) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives."	X			X	N/A - Backup media not released to public. Hardware outside accreditation boundary.
Confidentiality	PEDI-1	Data Interception	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.	X	X			MET - DOEHRS DR is housed in a secure area; addressed in the SSAA; however DOEHRS DR relies upon the MTFs for workstation security. This control is a site accreditation issue at the

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review				Comment
					I	D	T	O	
									MTFs
Availability	PEEL-2	Emergency Lighting	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes	X	X			MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PEFD-2	Fire Detection	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	X	X			MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PEFI-1	Fire Inspection	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	X	X			MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PEFS-2	Fire Suppression System	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke or particles.	X	X			MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Test	Review					Comment
					I	D	T	O	N	
Availability	PEHC-2	Humidity Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.	X	X				MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PEMS-1	Master Power Switch	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.	X	X				MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Confidentiality	PEPF-1	Physical Protection of Facilities	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.	X					MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue.
Confidentiality	PEPS-1	Physical Security Testing	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.	X					MET - Addressed in the SSAA; however DOEHRs DR partially relies upon CHPPM @ Aberdeen for PHYSEC. This control is also a site accreditation issue
Integrity	PESL-1	Screen Lock	DoDI 8500.2, 6	Unless there is an overriding technical	X	X				MET - Addressed in the

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
			Feb 03, Encl. 4, Attach. 2.	or operational problem, a workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).						SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Confidentiality	PESP-1	Workplace Security Procedures	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.	X	X				MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Confidentiality	PESS-1	Storage	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.	X					MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Availability	PETC-2	Temperature Controls	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.	X					MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PETN-1	Environmental Control Training	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Employees receive initial and periodic training in the operation of environmental controls.	X					PARTIALLY MET - However, DOEHRs DR relies on CHPPM @ Aberdeen for PHYSEC. Training on environmental controls not located in SSAA. This control is a site accreditation issue and is not deemed a finding for this C&A
Confidentiality	PEVC-1	Visitor Control to Computing Facilities	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.	X	X				MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue
Availability	PEVR-1	Voltage Regulators	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Automatic voltage control is implemented for key IT assets.	X	X				MET - Addressed in the SSAA; however DOEHRs DR relies upon CHPPM @ Aberdeen for PHYSEC. This control is a site accreditation issue

For Official Use Only

DOEHR-S-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Security Design and Configuration										
Availability	DCAR-1	Procedural Review	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.		X				MET - Annual Review in 2003
Confidentiality	DCAS-1	Acquisition Standards	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources – the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program.	X		X			MET – Oracle 8i, Oracle 9i evaluated COTS
				Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also						accreditation issue

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Integrity	DCBP-1	Best Security Practices	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.	X	X	X	X	X	MET – Best security available through DoD at this time
Integrity	DCCB-2	Control Board	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	All information systems are under the control of a chartered Configuration Control Board that meets regularly according to DCPR-1. The IAM is a member of the CCB.	X					MET - PITPO has CCB Charter and CMMIP
Integrity	DCCS-2	Configuration Specifications	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a Departmental reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a DoD reference guide.	X					MET - TFM in SSAA; STIGS applied
Availability	DCCT-1	Compliance Testing	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	X	X				MET
Integrity	DCDS-1	Dedicated IA	DoDI 8500.2, 6 Feb 03, Encl. 4,	Acquisition or outsourcing of dedicated IA services such as incident	X	X				MET - DOEHRS repository at CHPPM;

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
		Services	Attach. 2.	monitoring, analysis and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.						application distributed to MTF or clinics; DAAs required to adhere to DITSCAP process, and accept site risk
Integrity	DCFA-1	Functional Architecture for AIS Applications	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	For AIS applications, a functional architecture that identifies the following has been developed and is maintained: - all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface. - user roles required for access control and the access privileges assigned to each role (See ECAN). - unique security requirements (e.g., encryption of key data elements at rest) - categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA) restoration priority of subsystems, processes, or information (See COEF).	X					MET – System Architecture Section of the SSA. HIPAA may become an issue in the next Annual Review
Availability	DCHW-1	HW Baseline	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the	X	X				MET – At least one inventory is maintained in CM library at RITPO, and is not collocated

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Integrity	DCID-1	Interconnection Documentation	DoD1 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	inventory is stored in a fire-rated container or otherwise not collocated with the original.			X			MET - This application presently is deployed. Only one hosting site; i.e. CHHP at APG
Integrity	DCII-1	IA Impact Assessment	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.	X					NOT MET – RITPO CCB in SSAA; no changes since system migration to RIPTO; however DOEHRs-DR migration from Oracle 8i to Oracle 9i is a major change without C&A consideration or notification to JMSO (Migration delayed to facilitate this C&A). Not designated as a risk at this time, but will be revisited at Annual Review

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
										Risk: LOW
Integrity	DCIT-1	IA for IT Services	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.	X	X				N/A – No outsourcing for DOEHRs DR. Project Plan between RITPO and CHPPM
Integrity	DCMC-1	Mobile Code	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements: (1) Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used. (2) Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited. (3) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used. (4) Category 2 mobile code that	X	X			X	N/A – No mobile code in DOEHRs DR

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					
					I	D	T	O	N	A
				does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., S/PPPNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate). (5) Category 3 mobile code may be used. (6) All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited. (7) The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.						
Integrity	DCNR-1	Non-repudiation	DODI 8500.2, 6 Feb 03, Encl. 4 Attach. 2.	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.	X					MET - Server PKI certificate; tokens not yet applicable to this DoD system
Integrity	DCPA-1	Partitioning the Application	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of	X	X				MET

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review						
					I	D	T	O	N	A	
				different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.							
Availability	DCPB-1	IA Program and Budget	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A discrete line item for Information Assurance is established in programming and budget documentation.					X		
Availability	DCPD-1	Public Domain Software Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware are not used in DOD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.				X		MET – No freeware or public domain software	
Availability	DCPP-1	Ports, Protocols, and Services	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	DOD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT		X				MET- Port 443 open	

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					
					I	D	T	O	N	Comment
Integrity	DCPR-1	CM Process	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.	X					MET – SSAA reflects CM process and CCB. No changes in DOEHRs DR since migration to RTPO from CITPO
Availability	DCSD-1	IA Documentation	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	All appointments to required IA roles, e.g., DAA and IAM/AO, are established in writing, to include assigned duties and appointment		X	X			MET

September 2004

For Official Use Only

B-56

For Official Use Only

DOEHRSDR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
				criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).						
Integrity	DCSL-1	System Library Management Controls	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.		X				MET – System libraries accessible only by System Administrators
Integrity	DCSP-1	Security Support Structure Partitioning	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.		X				MET – Permissions are set
Integrity	DCSQ-1	Software Quality	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development		X				MET

For Official Use Only

DOEHRSDR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Confidentiality	DCSR-2	Specified Robustness – Medium	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 5.	At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.			X			MET – Sensitive information protected
Integrity	DCSS-2	System State Changes	DODI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.	X					MET
Availability	DCSW-1	SW Baseline	DODI 8500.2, 6	A current and comprehensive baseline	X	X				MET by documentation

September 2004

For Official Use Only

B-58

For Official Use Only

DOEHRS-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
Vulnerability and Incident Management										
Availability	VIIR-1	Incident Response Planning	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.	X	X				MET - Addressed in the SSAA; however DOEHRS DR relies upon CHPPM® Aberdeen for PHYSEC and incident responses. This control is a site accreditation issue
Availability	VIVM-1	Vulnerability Management	DoDI 8500.2, 6 Feb 03, Encl. 4, Attach. 2.	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have	X	X				MET - VMS registered

For Official Use Only

DOEHRs-DR 1.5.1 Certification and Accreditation Report

IA Service	IA Control #	IA Control Name	Source	IA Control Text	Review					Comment
					I	D	T	O	N	
				been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.						

September 2004

B-60

For Official Use Only